

C05100891

Approved for Release: 2017/07/12 C05100891
~~SECRET//NOFORN~~ ^{Unclassified}

National Reconnaissance Office

Business Function 80, Oversight

Directive 80-4,

(b)(3)



15 NOVEMBER 2012

CL BY:
DECL ON: 20390704
DRV FROM: INCG 1.0, 13 Feb 2012

(b)(3)

~~SECRET//NOFORN~~ ^{Unclassified}
Approved for Release: 2017/07/12 C05100891

ND 80-4
FY 2012

TABLE OF CONTENTS

(U) ND 80-4 CHANGE LOG	3
(U) SECTION I - INTRODUCTION.....	4
(U) SECTION II - APPLICATION.....	4
(U) SECTION III - REFERENCES/AUTHORITIES.....	4
(U) SECTION IV - POLICY.....	5
(U) SECTION V - ROLES AND RESPONSIBILITIES.....	8
(U) SECTION VI - DIRECTIVE POINT OF CONTACT.....	11
(U) APPROVING SIGNATURE.....	11
(U) APPENDIX - GLOSSARY and ABBREVIATION LIST.....	11

ND 80-4,
FY 2012

(U) ND 80-4 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks
VERSION 1	8/14/2014		ALL	ADMINISTRATIVE UPDATES BASED ON CHANGE OF CHAIR FROM BPO AND RELATED PROCESS ADJUSTMENTS

(b)(

ND 80-4,
FY 2012

(b)(1)

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, this NRO Directive (ND) defines the scope, authorities, and responsibilities specific to NRO Business Function (NBF) 80, Oversight. The ND is coordinated with appropriate stakeholders, and approved by the NBF owner, with administrative approval of the Director, Office of Policy and Strategy (OP&S). OP&S archives these official records.

(U) SECTION II - APPLICATION

(U) All personnel who are assigned or detailed to the NRO and who perform tasks or have duties specific to NBF 80 will comply with this ND and its corresponding instructions. When work under an NRO contract must comply with this directive and corresponding instructions, the program office shall list those as reference documents in the contract statement of work.

(U) SECTION III - REFERENCES/AUTHORITIES

- a. (U) NBF 80, Oversight, 4 April 2014;
- b. (U) NBF 60, Mission Operations, 3 April 2012;
- c. (U) ND 100-35, NRO RESERVE Control System, 26 April 2013;
- d. (U) DCI Directive 6/11, "Controlled Access Program Oversight Committee," 14 November 2002;
- e. (U) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010;
- f. (U) DoD Directive S-5105.61, "Department of Defense Cover and Cover Support Activities," May 6, 2010;
- g. (U) DoD Directive S-5210.36, "Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government," November 6, 2008;
- h. (U) DNRO Memo, "Delegation of National Reconnaissance Office Official Cover Plan Approval Authority," 25 July 2012; and

(b)(3)

ND 80-4,
FY 2012

(b)

(U) SECTION IV - POLICY

(U) It is the policy of the NRO to conduct all NRO support to sensitive activities in full compliance with applicable laws, regulations, and executive branch policy and in full conformity with external notification and cross-agency coordination requirements. [redacted]

(b)(3)

is the Director, NRO's (DNRO) corporate oversight mechanism for such activities and is the primary advisory body to the DNRO in the sensitive activities area.

(U) Consistent with DNRO policy and direction, the [redacted] serves as an oversight body with authority to approve or disapprove activities or refer them to the DNRO for approval as appropriate. The Chair of the [redacted] determines which activities and decisions are approved at the [redacted] level and which must be referred to the DNRO. The DNRO and the Principal Deputy Director, NRO (PDDNRO) are the only officials who can exempt activities deemed as sensitive from [redacted] review and oversight.

(b)(3)

(U) The [redacted] is responsible for reviewing internal requests to initiate new sensitive activities or relationships, external requests for support, and monitoring the status of previously approved activities. The [redacted] is also responsible for independently assessing proposed program protection plans and for reviewing and providing a recommendation to the DNRO on Office of Security and Counterintelligence (OS&CI) recommendations for NRO RESERVE or other security compartment requests requiring DNRO approval.

(b)(3)

(U) All Directorates and Offices (Ds and Os) are required to coordinate sensitive activities with the [redacted] prior to providing support or initiating activities. Ds and Os are also required to keep the [redacted] currently informed during the execution phase on a schedule agreed upon by the [redacted] and the activity manager.

(b)(3)

(U) Sensitive Activities

(U) Guidelines defining sensitive activities are provided below. The DNRO and [redacted] Chair determine if proposed programs, projects or activities fall under the purview of the [redacted]. Sensitive activities include but are not limited to:

(b)(3)

a. (U) Activities, operations, or programs requiring special compartmentation, restricted access, or program-unique information handling protections, i.e., NRO RESERVE, Department

ND 80-4,
FY 2012

(b)(

of Defense (DoD) Special Access Program (SAP) or Intelligence Community (IC) Controlled Access Program (CAP) protections;

(b)(1)
(b)(3)

c. (U) Requests for sensitive support originating from outside established channels;

(b)(1)
(b)(3)(b)(1)
(b)(3)(b)(3)
(b)(1)

g. (U) Activities involving or likely to result in the development of law enforcement information;

h. (U) All tests of NRO sensitive activities within the U.S. contiguous and non-contiguous states;

i. (U) All tests of NRO sensitive activities in U.S. territories;

j. (U) All NRO test activities outside of the United States and its territories, whether they are sensitive activities or not. This includes any test that involves NRO personnel or NRO equipment at that location, whether deployed or not, for the purposes of the test;

k. (U) Vulnerability and End-of-Life tests for all NRO satellites, as defined in NBF-60, Operations;

l. (U) Activities that could reveal or compromise sensitive sources and methods;

m. (U) Efforts that would put NRO personnel at risk;

n. (U) Activities that could result in the inadvertent collection against U.S. citizens or result in a perceived collection against U.S. citizens as directed under E.O. 12333;

ND 80-4,
FY 2012

(b)(

o. (U) Activity that is prohibited by Intelligence Community or Department of Defense policy, requiring approval at the senior community level; and

p. (U) Any activity so designated by the DNRO, PDDNRO or [] Chair.

(b)(3)

(U) Anything associated with or resulting from NRO support to sensitive activities that requires senior leadership awareness or action must be reported as soon as possible to the Chair of the []

(b)(3)

(U) Membership

(U) The DNRO appoints the Chair of the [] and all [] members. The Chair is solely responsible for the management of the [] consistent with DNRO direction and priorities. The Chair is also responsible for keeping the DNRO and PDDNRO currently informed of all [] activities, discussions, and recommendations.

(b)(3)

(U) The DNRO has appointed the following senior managers to serve as members of the [] Each senior manager listed below is allowed one alternate, who must be approved by the DNRO.

(b)(3)

a. (U) Director, Office of Policy and Strategy (OP&S), who will serve as Chair of the []

(b)(3)

b. (U) NRO General Counsel (GC);

c. (U) Director, Advanced Systems and Technology Directorate;

d. (U) Director, Chief Information Office

e. (U) Director, Ground Enterprise Directorate;

f. (U) Director, Mission Integration Directorate;

g. (U) Director, Mission Operations Directorate;

h. (U) Director, Office of Security and Counterintelligence;

i. (U) Director, Survivability Assurance Office;

j. (U) Director, Special Communications Office; and

k. (U) Director, Systems Engineering Directorate.

ND 80-4, [REDACTED]
FY 2012

(b)(

(U) The DNRO has approved the following supporting personnel to participate at the discretion of the Chair:

a. (U) [REDACTED]

(b)(3)

b. (U) [REDACTED]

c. (U) [REDACTED]

Executive Secretary;

d. (U) [REDACTED]

e. (U) [REDACTED]

f. (U) Other Ds and Os, Programs, and Activities as necessary.

(U) Executive Secretary and general secretariat support for the [REDACTED] are provided by OP&S within existing directorate staffing and funding levels consistent with the direction of the Chair.

(b)(3)

(U) SECTION V - ROLES AND RESPONSIBILITIES

(U) Director, OP&S

a. (U) Chair the [REDACTED]

(b)(3)

b. (U) Convey DNRO policy and direction to the [REDACTED]

(b)(3)

c. (U) Facilitate [REDACTED] meetings, ensure thorough consideration of topics, assign actions and establish due dates;

(b)(3)

d. (U) Review and approve [REDACTED] meeting minutes;

(b)(3)

e. (U) Review and approve recommendations to the DNRO for specifically designated groups to obtain and utilize NRO compartmented information for defined purposes;

f. ~~(S//NF)~~ Approve all NRO [REDACTED]

(b)(1)

(b)(3)

g. (U) Conduct an annual review of all RESERVE compartments; and

h. (U) Review and approve all NRO sensitive activities that meet the reporting thresholds identified in Section IV, above.

ND 80-4,
FY 2012

(b)

(U) NRO GC

(U) Ensure [] decisions and recommendations to the DNRO are in full compliance with applicable laws, regulations, and executive branch policy and are in full conformity with external notification and cross-agency coordination requirements.

(b)(1)

(U) Other Senior Managers serving as [] Members

(b)(3)

a. (U) Attend [] meetings or ensure that the designated alternate representative attends;

(b)(3)

b. (U) Be prepared to present, discuss, and make recommendations on agenda items;

c. (U) Complete action items and report on assigned issues by established deadlines;

d. (U) Coordinate issues across respective Directorate or Office;

e. (U) Present D or O concerns and interests; and

f. (U) Review and approve [] meeting minutes.

(b)(3)

(U) []

(b)(3)

a. (U) Serve as a non-voting member to provide technical and program management support to the []

(b)(3)

b. (U) Serve as the NRO focal point to coordinate and de-conflict SAPs, RESERVE compartments, and other sensitive activities supported by the NRO;

c. (U) Produce and brief the annual report to the Office of the Undersecretary of Defense for Intelligence Special Access Programs Coordination Office (OUSD(I) SAPCO); and

d. (U) Produce and brief the annual report to the Office of the Director of National Intelligence Controlled Access Programs Management Division (CAPMD) Senior Review Group (ODNI CAPMD/SRG).

ND 80-4,
FY 2012

[REDACTED]

(b)

(U) [REDACTED]

a. (U) Serve as a non-voting member to provide security support to the [REDACTED]

b. (U) Serve as the NRO control officer for external SCI control systems;

c. (U) Establish and maintain RESERVE Control System and compartment processes and templates; and

d. (U) Assist the [REDACTED] in producing the annual reports to the OUSD(I) SAPCO and the ODNI CAPMD/SRG.

(b)(3)

(U) [REDACTED] **Executive Secretary**

a. (U) Serve as a non-voting member to provide administrative and logistical support to the [REDACTED]

b. (U) Provide organizational and technical support to the [REDACTED] Chair and [REDACTED] to help assess and resolve issues; and

(b)(3)

c. (U) Serve as the [REDACTED] Records Control Officer.

(b)(3)

(U) [REDACTED]

a. (U) The [REDACTED] is composed of a core group and non-core group and is co-chaired by the [REDACTED]

(b)(3)

b. (U) The core group is composed of the [REDACTED] and [REDACTED] Executive Secretary; and

(b)(3)

c. (U) The non-core group is composed of representatives from the NRO [REDACTED] Office of General Counsel, OP&S, Counterintelligence, [REDACTED] and other experts as needed.

(b)(3)

d. (U) Staff sensitive activity issues for the [REDACTED] Chair;

(b)(3)

e. (U) Screen tests requiring [REDACTED] review and recommend to the [REDACTED] Chair the tests that the [REDACTED] Chair could approve and ones that should receive full [REDACTED] review.

(b)(3)

ND 80-4,
FY 2012

(b)(3)

(U)

(b)(3)

a. (U) Facilitate [] test event coordination and sensitive activity oversight responsibilities and functions;

(b)(3)

b. (U) Ensure test and sensitive activity approval processes and procedures are consistent, reported and easily understood; and

c. (U) Maintain a database of test events and activities.

(U) Other Ds and Os, Programs, and Activities

(U) Prepare, coordinate, and deconflict sensitive activity topics with the [] Executive Secretary prior to [] engagement.

(b)(3)

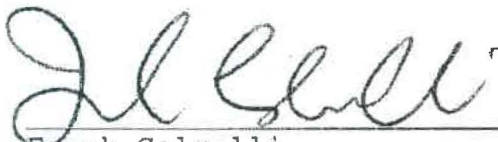
(U) SECTION VI - DIRECTIVE POINT OF CONTACT

(U) Chair, [] Director, BPO, [].

(b)(3)

(U) APPROVING SIGNATURE

(U) As the NBF owner for NBF 80, Oversight, I confirm that this document provides a complete representation of the ND 80-4, SAMB, and the document has been coordinated with stakeholders in this process.



Frank Calvelli
Oversight NBF Owner

11/14/12
Date



Damon R. Wells
Director, Office of Policy
and Strategy

11/15/12
Date

(b)(3)

(U) APPENDIX - GLOSSARY and ABBREVIATION LIST

ND 80-4, [REDACTED]
FY 2012

(b)(1)

Table is U//~~FOUO~~

(U) Term and Abbreviation	(U) Definition
Controlled Access Program (CAP)	(U) An IC compartmented program.
Controlled Access Program Management Division (CAPMD)	(U) The IC office responsible for oversight and management of all IC controlled access programs and oversight and management of the IC's classification and control markings system as defined in ICD 710.
Intelligence Community Policy Guidance (ICPG)	(U) ICPGs are ODNI policy instruments that establish policy and guidance and provide formal and definitive direction to the IC for the purposes of achieving a unified, integrated, and effective IC.
[REDACTED]	(U) The NRO body that serves as an oversight body with authority to approve or disapprove activities or refer them to the DNRO for approval as appropriate.
[REDACTED]	(U) An arm of the [REDACTED] composed of the [REDACTED] Executive Secretary, and other experts as needed, whose role is to staff sensitive activity issues for the [REDACTED] Chair.
Special Access Program (SAP)	(U) A DoD compartmented program.
Special Access Program Coordination Office (SAPCO)	(U// FOUO) The DoD office that manages DoD SAPs and provides management and direction DoD and other U.S. Government SAPs.
[REDACTED]	(U) A non-voting member of the [REDACTED] who provides program insight and advice, and assists in de-conflicting special activities.
[REDACTED]	(U) A non-voting member of the [REDACTED] who provides security support, coordination, and advice, and serves as cross-agency liaison for sensitive activities.
[REDACTED]	(U) An arm of the [REDACTED] that coordinates and oversees NRO test events and manages the [REDACTED] using the [REDACTED] (NI 80-4-2).

(b)(3)

(b)(3)

(b)(3)

(b)(3)

Table is U//~~FOUO~~

(U) National Reconnaissance Office

(U) Business Function 80, Oversight
(U) Directive 80-7, Signals Intelligence Compliance



27 JANUARY 2014

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) TABLE OF CONTENTS

(U) ND 80-7 CHANGE LOG	3
(U) SECTION I - INTRODUCTION.....	4
(U) SECTION II - APPLICATION.....	4
(U) SECTION III - REFERENCES/AUTHORITIES.....	4
(U) SECTION IV - POLICY.....	5
(U) SECTION V - ROLES AND RESPONSIBILITIES.....	7
(U) SECTION VI - DIRECTIVE POINT OF CONTACT.....	8
(U) APPROVING SIGNATURE.....	9
(U) APPENDIX A - ACRONYM LIST.....	10
(U) APPENDIX B - GLOSSARY.....	11

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) ND 80-7 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks
0	27 June 2012	Office of Policy and Strategy		Initial release as Office of the Director Policy Note 2012-05
1.0	27 January 2014	Office of Policy and Strategy	All	First release as a National Reconnaissance Office Directive

Table is UNCLASSIFIED

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, this NRO Directive (ND) defines scope, authorities, and responsibilities specific to NRO Business Function (NBF) 80. The ND is coordinated with appropriate stakeholders, and is approved by the NBF Owner, with administrative approval of the Director, Office of Policy and Strategy (OP&S). Official record copies are archived by OP&S.

(U) This directive rescinds Office of the Director Policy Note 2012-05, *National Reconnaissance Office Signals Intelligence Compliance*, dated 27 June 2012.

(U) SECTION II - APPLICATION

(U) All NRO personnel who have duties requiring access to raw or unminimized signals intelligence (SIGINT) data or manage those who require access shall comply with this ND and its corresponding instructions.

(U) This directive establishes foundational policy for the NRO SIGINT Compliance Program. The SIGINT Compliance Program was established to ensure that the NRO complies with all applicable laws, Executive Orders (E.O.s), and directives related to the use of SIGINT data by NRO personnel. This policy is applicable to all NRO-assigned personnel regardless of work location (government or contractor facility) who have access to, or handle, raw or unminimized NRO-acquired SIGINT data.

(U) When work performed under an NRO contract requires access to raw or unminimized SIGINT data, all contractor personnel who access or may have access to that data must comply with the contractual requirements regarding the NRO SIGINT Compliance Program. The applicable NRO program office shall list this directive and corresponding instructions as reference documents in the contract statement of work.

(U) SECTION III - REFERENCES/AUTHORITIES

- a. (U) NRO Governance Plan, 25 October 2011.
- b. (U) NRO Business Function 80, *Oversight*, 27 April 2012.
- c. (U) Executive Order 12333, United States Intelligence Activities, as amended 30 July 2008.

(U) ND 80-7, *Signals Intelligence Compliance*
FY 2014

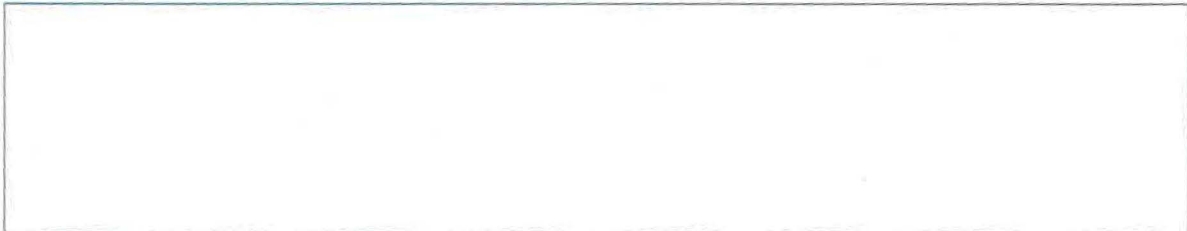
d. (U) Department of Defense 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.

e. (U) Directive-Type Memorandum (DTM) 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, 21 August 2013.

f. (U) National Security Council Intelligence Directive (NSCID) No. 6, *Signals Intelligence*, 17 February 1972.

g. (U) National Security Agency/Central Security Service (NSA/CSS) Policy 1-23, *Procedures Governing NSA/CSS Activities that Affect U.S. Persons*, 29 May 2009.

h. (U) United States Signals Intelligence Directive (USSID)/SP0018, *Legal Compliance and U.S. Persons Minimization Procedures*, 25 January 2011.



(b)(3)

j. (U//~~FOUO~~) Office of the Director Announcement Number 2011-38, *National Reconnaissance Office Signals Intelligence Compliance Officer*, 16 September 2011.

(U) SECTION IV - POLICY

(U//~~FOUO~~) The NRO shall facilitate the United States SIGINT mission in accordance with the following:

a. (U//~~FOUO~~) The Director, National Security Agency (DIRNSA), as the SIGINT Functional Manager, is legally responsible for the collection, processing, analysis, and dissemination of SIGINT.



(b)(3)

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

1. (U) The use of this data for any other purpose or its distribution beyond approved and properly trained NRO personnel is not authorized.

(b)(3)

(b)(3)

(b)(3)

e. ~~(U//FOUO)~~ This data shall be handled in a manner that protects information until the data has been properly minimized or conforms to the established handling and protection criteria for tasked SIGINT (Communications Intelligence, Electronic Intelligence, Foreign Instrumentation Intelligence or SIGINT Search) collection or other applicable non-SIGINT rules.

(b)(3)

f. ~~(U//FOUO)~~ NRO personnel requiring access to NRO-acquired SIGINT data for the performance of their duties shall have proper authorization, completed appropriate SIGINT compliance training, and a verified method of protecting the data, prior to accessing the SIGINT data. Protection of this data and adherence to this policy is required throughout the data life cycle.

(b)(3)

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) SECTION V - ROLES AND RESPONSIBILITIES

(U) Office of Policy and Strategy shall:

a. (U) Establish and maintain a SIGINT Compliance Group to implement and conduct the NRO's SIGINT Compliance Program;

b. (U) Coordinate with the NRO Office of General Counsel and [REDACTED] on matters related to SIGINT Compliance, as needed; (b)(3)

c. (U) Coordinate with the NRO Intelligence Oversight Program Manager on SIGINT-related Oversight and Compliance incident reporting;

d. (U) Establish and maintain NRO's SIGINT Compliance policy;

e. (U) Oversee the SIGINT Compliance Program across the NRO to ensure consistency with established policy;

f. (U) Ensure NRO compliance with applicable legislation, regulation, and Executive Branch policy;

g. (U) Develop, promulgate, and maintain program documentation providing additional guidance and information, as needed;

h. (U) Develop, promulgate, and maintain NRO SIGINT Compliance training materials;

i. (U) Monitor and audit the NRO for SIGINT Compliance on a regular basis; and

j. (U) Develop, approve, and sign appropriate implementing NRO Instructions under ND 80-7 to support the SIGINT Compliance Program.

(U) NRO Directorates and Offices shall:

a. (U) Comply with established NRO SIGINT Compliance policy;

b. (U) Execute SIGINT Compliance consistent with approved policy and training; and

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

c. (U) Appoint a [] to support the NRO's SIGINT Compliance Program and oversee compliance within the component, as applicable.

(b)(3)

(U) SECTION VI - DIRECTIVE POINT OF CONTACT

(U) Chief, [] Office of Policy and Strategy, [] .

(b)(3)

~~Unclassified~~Approved for Release: 2017/07/12 C05100892 ~~USE ONLY~~

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) APPROVING SIGNATURE


(U) As the Owner of NBF 80, Oversight, I confirm that this document provides a complete representation of ND 80-7, Signals Intelligence Compliance, and the document has been coordinated with stakeholders in this process.



Frank Calvelli
Oversight NBF Owner

1/27/14
Date



 Damon R. Wells
Director, Office of
Policy and Strategy

1-27-14
Date

(b)(3)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Approved for Release: 2017/07/12 C05100892

~~Unclassified~~

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) APPENDIX A - ACRONYM LIST

Acronym or Term	Definition
COMINT	Communications Intelligence
DIRNSA	Director, National Security Agency
DoD	Department of Defense
DTM	Directive-Type Memorandum
ELINT	Electronic Intelligence
E.O.	Executive Order
FISINT	Foreign Instrumentation Intelligence
NBF	National Reconnaissance Office Business Function
ND	National Reconnaissance Office Directive
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
NSCID	National Security Council Intelligence Directive
OP&S	Office of Policy and Strategy
SIGINT	Signals Intelligence
SP	Signals Intelligence Production
USSID	United States Signals Intelligence Directive

(b)(3)
(b)(3)

Table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) ND 80-7, Signals Intelligence Compliance
 FY 2014

(U) APPENDIX B - GLOSSARY

Acronym or Term	Definition
Communications Intelligence (COMINT)	(U) A subset discipline of signals intelligence (SIGINT) that refers to technical and intelligence information derived from the acquisition of foreign communications by the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means or the processing of foreign encrypted communications, however transmitted.
Data Life Cycle	(U) The end-to-end status of SIGINT data from acquisition of radio frequency signal, through processing, distribution, storage, and deletion and purging of the data.
Electronic Intelligence (ELINT)	(U) A subset discipline of SIGINT that refers to, technical and intelligence information derived from foreign non-communications electromagnetic emissions, primarily radars, emanating from other than nuclear detonations or radioactive courses. ELINT consists of two types: Operational ELINT and Technical ELINT.
Foreign Instrumentation Intelligence (FISINT)	(U) A subset discipline of SIGINT that refers to technical and intelligence information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational use of foreign aerospace, surface, and sub-surface systems. FISINT includes telemetry, beaconing, electronic interrogators, and video data links.
Minimization	(U//FOUO) Specific SIGINT procedures that, considering the purpose and technique of the particular surveillance, lessen the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. Persons consistent with the U.S. need to obtain, produce, and disseminate foreign intelligence and counterintelligence information.
Raw SIGINT	(U) SIGINT data collected either as a result of search and development or targeted collection operations against a particular foreign intelligence target before the information has been evaluated for foreign intelligence AND minimized to protect U.S. Person data.
Signals Intelligence (SIGINT)	(U) A category of intelligence comprising, either individually or in combination, COMINT, ELINT, and FISINT, however transmitted. In addition, SIGINT is intelligence derived from communications, electronic, and foreign instrumentation signals.

(b)(3)

Table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED

NATIONAL RECONNAISSANCE OFFICE14675 Lee Road
Chantilly, VA 20151-1715**Office of the Director Policy Note**

Number 2015-01

23 January 2015

PRESIDENTIAL POLICY DIRECTIVE 28 PROCEDURES**I. Introduction**

Presidential Policy Directive 28 (PPD-28) regarding signals intelligence activities issued 17 January 2014, sets forth principles to guide why, whether, when, and how the United States (U.S.) conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes. In particular, Section 4 of PPD-28 articulates principles for safeguarding personal information collected from signals intelligence activities and requires Intelligence Community (IC) elements to establish policies and procedures to apply these principles, in a manner consistent with technical capabilities and operational needs. This document constitutes the PPD-28 policies and procedures of the National Reconnaissance Office (NRO).

NRO is a joint Department of Defense (DoD) - IC organization responsible for developing, launching, and operating the United States' signals, imagery, and communications intelligence satellites. Data collected by NRO on behalf of the National Security Agency (NSA), National Geospatial-Intelligence Agency, and other NRO Mission Partners is used by these Mission Partners to produce intelligence products for the President, congress, national policy makers, warfighters, and civil users.

II. General Provisions and Authorities

NRO is an element of the IC pursuant to Section 3.5(h) of Executive Order 12333, as amended.

Pursuant to Section 1.7(d) of Executive Order 12333, as amended, NRO is to "be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs."

III. Safeguarding Personal Information Collected through Signals Intelligence

The following policies and procedures apply to NRO's safeguarding of personal information of non-U.S. persons collected through signals intelligence activities.¹

¹ These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act, Executive Order 12333, Bureau of Intelligence and Research's (INR) guidelines approved by the Attorney General pursuant to Sec. 2.3 of Executive Order 12333, or other applicable law.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Presidential Policy Directive 28 Procedures

a. *Minimization*

Although NRO has access to unevaluated and unminimized signals intelligence, it transfers such data to NSA for processing, evaluation, and minimization in accordance with NSA procedures. NRO also conducts research, development, test, and evaluation to enhance NSA's signals intelligence processing capabilities. In addition, NRO receives from other IC elements signals intelligence information that has been evaluated, minimized, or otherwise included in finished intelligence products subject to - among other requirements - the provisions of PPD-28.²

1. *Dissemination*³

NRO will disseminate personal information of non-U.S. persons collected through signals intelligence activities only if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333. NRO will disseminate personal information concerning a non-U.S. person that is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign status. Unless it possesses specific information to the contrary, NRO will presume that any evaluated or minimized signals intelligence information it receives from other IC elements meets these standards. NRO will disseminate such information in accordance with applicable policies and procedures.

2. *Retention*

NRO will retain personal information of non-U.S. persons collected through signals intelligence activities only if retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333. NRO will retain personal information concerning a non-U.S. person that is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign status. Unless it possesses specific information to the contrary, NRO will presume that any evaluated

² Such PPD-28 provisions include those in Section 1, such as (i) the U.S. shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; (ii) signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national or departmental missions and not for any other purposes; (iii) it is not an authorized foreign intelligence or counterintelligence purpose to collect foreign private commercial information or trade secrets to afford a competitive advantage to U.S. companies and U.S. business sectors commercially; and (iv) signals intelligence activities shall be as tailored as feasible. If INR suspects that signals intelligence disseminated to it may have been collected or disseminated in a manner inconsistent with PPD-28, it shall so notify appropriate officials at the IC element that disseminated the signals intelligence.

³ Dissemination is the transmission, communication, sharing, or passing of information by any means, including oral, electronic, or physical means.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Presidential Policy Directive 28 Procedures

or minimized signals intelligence information it receives from another IC element meets these standards. NRO will retain such information in accordance with applicable record retention policies.

b. Data Security and Access

Access to personal information of both U.S. and non-U.S. persons collected through signals intelligence activities - when identifiable - is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of NRO's mission. Such information will be maintained in either electronic or physical form in secure facilities protected by physical and technological safeguards, and with access limited by appropriate security measures. Such information will be safeguarded in accordance with applicable laws, rules, and policies, including those of NRO, the DoD, and the IC.

Classified information will be stored appropriately in a secured, certified, and accredited facility, in secured databases or containers, and in accordance with other applicable requirements. The NRO electronic system in which such information may be stored will comply with applicable law, Executive Orders, DoD, IC, and NRO policies and procedures regarding information security, including with regard to access controls and monitoring.

c. Data Quality

Personal information of both U.S. and non-U.S. persons collected through signals intelligence activities - when identifiable - shall be deleted as consistent with applicable NRO, DoD, and IC standards. Particular care should be taken to ensure only the technical characteristics of the data shall be retained as consistent with NRO's mission and applicable NRO, DoD, and IC standards.

d. Oversight

The NRO Signals Intelligence Compliance Officer (SCO) within NRO shall review implementation of these policies and procedures annually and report to the Office of General Counsel/Intelligence Oversight (OGC/IO), regarding the application of the safeguards contained herein and in Section 4 of PPD-28 more generally, as applicable.

Instances of non-compliance with these policies and procedures shall be reported to the NRO SCO and OGC/IO. NRO SCO and OGC/IO, in consultation with the Office of Inspector General (OIG), Office of the Deputy Chief Management Officer, and the Director of National Intelligence (DNI), as appropriate, shall determine what, if any, corrective actions are necessary and appropriate.

Significant instances of non-compliance with these policies and procedures involving the personal information of any person collected through signals intelligence activities shall be reported promptly to the NRO SCO and OGC/IO, who in turn will report them to the DNI pursuant to Section 4 of PPD-28.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Presidential Policy Directive 28 Procedures

IV. Training

NRO personnel whose duties require access to personal information collected through signals intelligence activities will receive annual training on the requirements of these policies and procedures.

V. Deviations from these Procedures

The NRO SCO must approve in advance any departures from these procedures, after consultation with the Office of the Director of National Intelligence and the National Security Division of the Department of Justice. If there is not time for such approval and a departure from these procedures is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the NRO SCO or the NRO SCO's senior representative present may approve a departure from these procedures. The Legal Adviser will be notified as soon thereafter as possible. The Legal Adviser will provide prompt written notice of any such departures to the Office of the Director of National Intelligence and the National Security Division of the Department of Justice. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

VI. Conclusion

These procedures are set forth solely for internal guidance within NRO. Questions on the applicability or interpretation of these procedures should be directed to Office of Policy and Strategy/Signals Intelligence Compliance Group and OGC/IO who, in consultation with the OIG, as appropriate, shall determine such applicability or interpretation.



Betty J. Sapp
Director

UNCLASSIFIED

(U) National Reconnaissance Office

(U) Business Function 80, Oversight
(U) Directive 80-7, Signals Intelligence Compliance



27 JANUARY 2014

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) TABLE OF CONTENTS

(U) ND 80-7 CHANGE LOG	3
(U) SECTION I - INTRODUCTION.....	4
(U) SECTION II - APPLICATION.....	4
(U) SECTION III - REFERENCES/AUTHORITIES.....	4
(U) SECTION IV - POLICY.....	5
(U) SECTION V - ROLES AND RESPONSIBILITIES.....	7
(U) SECTION VI - DIRECTIVE POINT OF CONTACT.....	8
(U) APPROVING SIGNATURE.....	9
(U) APPENDIX A - ACRONYM LIST.....	10
(U) APPENDIX B - GLOSSARY.....	11

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) ND 80-7 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks
0	27 June 2012	Office of Policy and Strategy		Initial release as Office of the Director Policy Note 2012-05
1.0	27 January 2014	Office of Policy and Strategy	All	First release as a National Reconnaissance Office Directive

Table is UNCLASSIFIED

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, this NRO Directive (ND) defines scope, authorities, and responsibilities specific to NRO Business Function (NBF) 80. The ND is coordinated with appropriate stakeholders, and is approved by the NBF Owner, with administrative approval of the Director, Office of Policy and Strategy (OP&S). Official record copies are archived by OP&S.

(U) This directive rescinds Office of the Director Policy Note 2012-05, *National Reconnaissance Office Signals Intelligence Compliance*, dated 27 June 2012.

(U) SECTION II - APPLICATION

(U) All NRO personnel who have duties requiring access to raw or unminimized signals intelligence (SIGINT) data or manage those who require access shall comply with this ND and its corresponding instructions.

(U) This directive establishes foundational policy for the NRO SIGINT Compliance Program. The SIGINT Compliance Program was established to ensure that the NRO complies with all applicable laws, Executive Orders (E.O.s), and directives related to the use of SIGINT data by NRO personnel. This policy is applicable to all NRO-assigned personnel regardless of work location (government or contractor facility) who have access to, or handle, raw or unminimized NRO-acquired SIGINT data.

(U) When work performed under an NRO contract requires access to raw or unminimized SIGINT data, all contractor personnel who access or may have access to that data must comply with the contractual requirements regarding the NRO SIGINT Compliance Program. The applicable NRO program office shall list this directive and corresponding instructions as reference documents in the contract statement of work.

(U) SECTION III - REFERENCES/AUTHORITIES

- a. (U) NRO Governance Plan, 25 October 2011.
- b. (U) NRO Business Function 80, *Oversight*, 27 April 2012.
- c. (U) Executive Order 12333, United States Intelligence Activities, as amended 30 July 2008.

(U) ND 80-7, *Signals Intelligence Compliance*
FY 2014

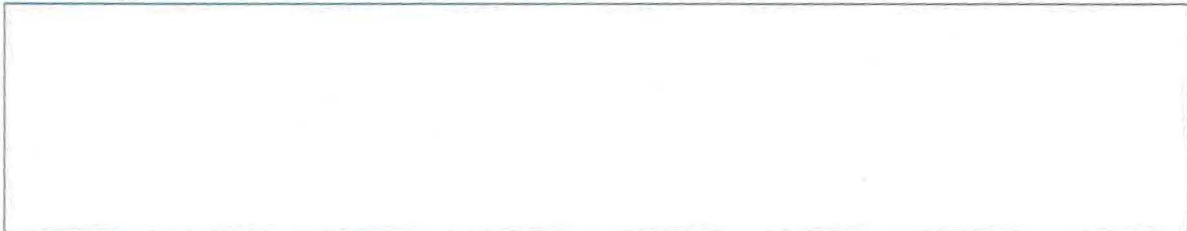
d. (U) Department of Defense 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.

e. (U) Directive-Type Memorandum (DTM) 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, 21 August 2013.

f. (U) National Security Council Intelligence Directive (NSCID) No. 6, *Signals Intelligence*, 17 February 1972.

g. (U) National Security Agency/Central Security Service (NSA/CSS) Policy 1-23, *Procedures Governing NSA/CSS Activities that Affect U.S. Persons*, 29 May 2009.

h. (U) United States Signals Intelligence Directive (USSID)/SP0018, *Legal Compliance and U.S. Persons Minimization Procedures*, 25 January 2011.



(b)(3)

j. ~~(U//FOUO)~~ Office of the Director Announcement Number 2011-38, *National Reconnaissance Office Signals Intelligence Compliance Officer*, 16 September 2011.

(U) SECTION IV - POLICY

~~(U//FOUO)~~ The NRO shall facilitate the United States SIGINT mission in accordance with the following:

a. ~~(U//FOUO)~~ The Director, National Security Agency (DIRNSA), as the SIGINT Functional Manager, is legally responsible for the collection, processing, analysis, and dissemination of SIGINT.



(b)(3)

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

1. (U) The use of this data for any other purpose or its distribution beyond approved and properly trained NRO personnel is not authorized.

(b)(3)

(b)(3)

(b)(3)

e. ~~(U//FOUO)~~ This data shall be handled in a manner that protects information until the data has been properly minimized or conforms to the established handling and protection criteria for tasked SIGINT (Communications Intelligence, Electronic Intelligence, Foreign Instrumentation Intelligence or SIGINT Search) collection or other applicable non-SIGINT rules.

(b)(3)

f. ~~(U//FOUO)~~ NRO personnel requiring access to NRO-acquired SIGINT data for the performance of their duties shall have proper authorization, completed appropriate SIGINT compliance training, and a verified method of protecting the data, prior to accessing the SIGINT data. Protection of this data and adherence to this policy is required throughout the data life cycle.

(b)(3)

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) SECTION V - ROLES AND RESPONSIBILITIES

(U) Office of Policy and Strategy shall:

a. (U) Establish and maintain a SIGINT Compliance Group to implement and conduct the NRO's SIGINT Compliance Program;

b. (U) Coordinate with the NRO Office of General Counsel and [REDACTED] on matters related to SIGINT Compliance, as needed; (b)(3)

c. (U) Coordinate with the NRO Intelligence Oversight Program Manager on SIGINT-related Oversight and Compliance incident reporting;

d. (U) Establish and maintain NRO's SIGINT Compliance policy;

e. (U) Oversee the SIGINT Compliance Program across the NRO to ensure consistency with established policy;

f. (U) Ensure NRO compliance with applicable legislation, regulation, and Executive Branch policy;

g. (U) Develop, promulgate, and maintain program documentation providing additional guidance and information, as needed;

h. (U) Develop, promulgate, and maintain NRO SIGINT Compliance training materials;

i. (U) Monitor and audit the NRO for SIGINT Compliance on a regular basis; and

j. (U) Develop, approve, and sign appropriate implementing NRO Instructions under ND 80-7 to support the SIGINT Compliance Program.

(U) NRO Directorates and Offices shall:

a. (U) Comply with established NRO SIGINT Compliance policy;

b. (U) Execute SIGINT Compliance consistent with approved policy and training; and

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

c. (U) Appoint a [] to support the NRO's SIGINT Compliance Program and oversee compliance within the component, as applicable.

(b)(3)

(U) SECTION VI - DIRECTIVE POINT OF CONTACT

(U) Chief, [] Office of Policy and Strategy, [] .

(b)(3)

~~Unclassified~~Approved for Release: 2017/07/12 C05100892 ~~USE ONLY~~

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) APPROVING SIGNATURE


(U) As the Owner of NBF 80, Oversight, I confirm that this document provides a complete representation of ND 80-7, Signals Intelligence Compliance, and the document has been coordinated with stakeholders in this process.



Frank Calvelli
Oversight NBF Owner

1/27/14
Date



 Damon R. Wells
Director, Office of
Policy and Strategy

1-27-14
Date

(b)(3)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Approved for Release: 2017/07/12 C05100892

~~Unclassified~~

(U) ND 80-7, Signals Intelligence Compliance
FY 2014

(U) APPENDIX A - ACRONYM LIST

Acronym or Term	Definition
COMINT	Communications Intelligence
DIRNSA	Director, National Security Agency
DoD	Department of Defense
DTM	Directive-Type Memorandum
ELINT	Electronic Intelligence
E.O.	Executive Order
FISINT	Foreign Instrumentation Intelligence
NBF	National Reconnaissance Office Business Function
ND	National Reconnaissance Office Directive
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
NSCID	National Security Council Intelligence Directive
OP&S	Office of Policy and Strategy
SIGINT	Signals Intelligence
SP	Signals Intelligence Production
USSID	United States Signals Intelligence Directive

Table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

(b)(3)
(b)(3)

(U) ND 80-7, Signals Intelligence Compliance
 FY 2014

(U) APPENDIX B - GLOSSARY

Acronym or Term	Definition
Communications Intelligence (COMINT)	(U) A subset discipline of signals intelligence (SIGINT) that refers to technical and intelligence information derived from the acquisition of foreign communications by the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means or the processing of foreign encrypted communications, however transmitted.
Data Life Cycle	(U) The end-to-end status of SIGINT data from acquisition of radio frequency signal, through processing, distribution, storage, and deletion and purging of the data.
Electronic Intelligence (ELINT)	(U) A subset discipline of SIGINT that refers to, technical and intelligence information derived from foreign non-communications electromagnetic emissions, primarily radars, emanating from other than nuclear detonations or radioactive courses. ELINT consists of two types: Operational ELINT and Technical ELINT.
Foreign Instrumentation Intelligence (FISINT)	(U) A subset discipline of SIGINT that refers to technical and intelligence information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational use of foreign aerospace, surface, and sub-surface systems. FISINT includes telemetry, beaconing, electronic interrogators, and video data links.
Minimization	(U// FOUO) Specific SIGINT procedures that, considering the purpose and technique of the particular surveillance, lessen the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. Persons consistent with the U.S. need to obtain, produce, and disseminate foreign intelligence and counterintelligence information.
Raw SIGINT	(U) SIGINT data collected either as a result of search and development or targeted collection operations against a particular foreign intelligence target before the information has been evaluated for foreign intelligence AND minimized to protect U.S. Person data.
Signals Intelligence (SIGINT)	(U) A category of intelligence comprising, either individually or in combination, COMINT, ELINT, and FISINT, however transmitted. In addition, SIGINT is intelligence derived from communications, electronic, and foreign instrumentation signals.

Table is UNCLASSIFIED//FOR OFFICIAL USE ONLY

(b)(3)

UNCLASSIFIED

NATIONAL RECONNAISSANCE OFFICE14675 Lee Road
Chantilly, VA 20151-1715**Office of the Director Policy Note**

Number 2015-01

23 January 2015

PRESIDENTIAL POLICY DIRECTIVE 28 PROCEDURES**I. Introduction**

Presidential Policy Directive 28 (PPD-28) regarding signals intelligence activities issued 17 January 2014, sets forth principles to guide why, whether, when, and how the United States (U.S.) conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes. In particular, Section 4 of PPD-28 articulates principles for safeguarding personal information collected from signals intelligence activities and requires Intelligence Community (IC) elements to establish policies and procedures to apply these principles, in a manner consistent with technical capabilities and operational needs. This document constitutes the PPD-28 policies and procedures of the National Reconnaissance Office (NRO).

NRO is a joint Department of Defense (DoD) - IC organization responsible for developing, launching, and operating the United States' signals, imagery, and communications intelligence satellites. Data collected by NRO on behalf of the National Security Agency (NSA), National Geospatial-Intelligence Agency, and other NRO Mission Partners is used by these Mission Partners to produce intelligence products for the President, congress, national policy makers, warfighters, and civil users.

II. General Provisions and Authorities

NRO is an element of the IC pursuant to Section 3.5(h) of Executive Order 12333, as amended.

Pursuant to Section 1.7(d) of Executive Order 12333, as amended, NRO is to "be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs."

III. Safeguarding Personal Information Collected through Signals Intelligence

The following policies and procedures apply to NRO's safeguarding of personal information of non-U.S. persons collected through signals intelligence activities.¹

¹ These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act, Executive Order 12333, Bureau of Intelligence and Research's (INR) guidelines approved by the Attorney General pursuant to Sec. 2.3 of Executive Order 12333, or other applicable law.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Presidential Policy Directive 28 Procedures

a. *Minimization*

Although NRO has access to unevaluated and unminimized signals intelligence, it transfers such data to NSA for processing, evaluation, and minimization in accordance with NSA procedures. NRO also conducts research, development, test, and evaluation to enhance NSA's signals intelligence processing capabilities. In addition, NRO receives from other IC elements signals intelligence information that has been evaluated, minimized, or otherwise included in finished intelligence products subject to - among other requirements - the provisions of PPD-28.²

1. *Dissemination*³

NRO will disseminate personal information of non-U.S. persons collected through signals intelligence activities only if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333. NRO will disseminate personal information concerning a non-U.S. person that is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign status. Unless it possesses specific information to the contrary, NRO will presume that any evaluated or minimized signals intelligence information it receives from other IC elements meets these standards. NRO will disseminate such information in accordance with applicable policies and procedures.

2. *Retention*

NRO will retain personal information of non-U.S. persons collected through signals intelligence activities only if retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333. NRO will retain personal information concerning a non-U.S. person that is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign status. Unless it possesses specific information to the contrary, NRO will presume that any evaluated

² Such PPD-28 provisions include those in Section 1, such as (i) the U.S. shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; (ii) signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national or departmental missions and not for any other purposes; (iii) it is not an authorized foreign intelligence or counterintelligence purpose to collect foreign private commercial information or trade secrets to afford a competitive advantage to U.S. companies and U.S. business sectors commercially; and (iv) signals intelligence activities shall be as tailored as feasible. If INR suspects that signals intelligence disseminated to it may have been collected or disseminated in a manner inconsistent with PPD-28, it shall so notify appropriate officials at the IC element that disseminated the signals intelligence.

³ Dissemination is the transmission, communication, sharing, or passing of information by any means, including oral, electronic, or physical means.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: Presidential Policy Directive 28 Procedures

or minimized signals intelligence information it receives from another IC element meets these standards. NRO will retain such information in accordance with applicable record retention policies.

b. *Data Security and Access*

Access to personal information of both U.S. and non-U.S. persons collected through signals intelligence activities - when identifiable - is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of NRO's mission. Such information will be maintained in either electronic or physical form in secure facilities protected by physical and technological safeguards, and with access limited by appropriate security measures. Such information will be safeguarded in accordance with applicable laws, rules, and policies, including those of NRO, the DoD, and the IC.

Classified information will be stored appropriately in a secured, certified, and accredited facility, in secured databases or containers, and in accordance with other applicable requirements. The NRO electronic system in which such information may be stored will comply with applicable law, Executive Orders, DoD, IC, and NRO policies and procedures regarding information security, including with regard to access controls and monitoring.

c. *Data Quality*

Personal information of both U.S. and non-U.S. persons collected through signals intelligence activities - when identifiable - shall be deleted as consistent with applicable NRO, DoD, and IC standards. Particular care should be taken to ensure only the technical characteristics of the data shall be retained as consistent with NRO's mission and applicable NRO, DoD, and IC standards.

d. *Oversight*

The NRO Signals Intelligence Compliance Officer (SCO) within NRO shall review implementation of these policies and procedures annually and report to the Office of General Counsel/Intelligence Oversight (OGC/IO), regarding the application of the safeguards contained herein and in Section 4 of PPD-28 more generally, as applicable.

Instances of non-compliance with these policies and procedures shall be reported to the NRO SCO and OGC/IO. NRO SCO and OGC/IO, in consultation with the Office of Inspector General (OIG), Office of the Deputy Chief Management Officer, and the Director of National Intelligence (DNI), as appropriate, shall determine what, if any, corrective actions are necessary and appropriate.

Significant instances of non-compliance with these policies and procedures involving the personal information of any person collected through signals intelligence activities shall be reported promptly to the NRO SCO and OGC/IO, who in turn will report them to the DNI pursuant to Section 4 of PPD-28.

UNCLASSIFIED

SUBJECT: Presidential Policy Directive 28 Procedures

IV. Training

NRO personnel whose duties require access to personal information collected through signals intelligence activities will receive annual training on the requirements of these policies and procedures.

V. Deviations from these Procedures

The NRO SCO must approve in advance any departures from these procedures, after consultation with the Office of the Director of National Intelligence and the National Security Division of the Department of Justice. If there is not time for such approval and a departure from these procedures is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the NRO SCO or the NRO SCO's senior representative present may approve a departure from these procedures. The Legal Adviser will be notified as soon thereafter as possible. The Legal Adviser will provide prompt written notice of any such departures to the Office of the Director of National Intelligence and the National Security Division of the Department of Justice. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

VI. Conclusion

These procedures are set forth solely for internal guidance within NRO. Questions on the applicability or interpretation of these procedures should be directed to Office of Policy and Strategy/Signals Intelligence Compliance Group and OGC/IO who, in consultation with the OIG, as appropriate, shall determine such applicability or interpretation.



Betty J. Sapp
Director

UNCLASSIFIED

National Reconnaissance Office
Business Function 80, Oversight
Directive 80-7, Signals Intelligence Compliance
Instruction 80-7-1, Signals Intelligence Compliance
Incident Reporting



24 JUNE 2015

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

TABLE OF CONTENTS

(U) NI 80-7-1 CHANGE LOG	3
(U) SECTION I - INTRODUCTION	4
(U) SECTION II - OVERSIGHT, SIGINT COMPLIANCE INCIDENT REPORTING	4
(U) Governing NBF.....	4
(U) Description.....	4
(U) Instruction Point of Contact.....	4
(U) Support Systems.....	5
(U) Process Narrative.....	5
(U) Process Flow Diagram.....	8
(U) Table 1: Risk & Internal Control Table.....	9
(U) SECTION III - CONFIGURATION CONTROL.....	9
(U) APPROVING SIGNATURE.....	9
(U) APPENDIX A - PROCESS FLOW DIAGRAM LEGEND.....	10
(U) APPENDIX B - ACRONYM LIST AND GLOSSARY.....	11
(U) APPENDIX C - REFERENCES/AUTHORITIES.....	13
(U) APPENDIX D - NRO SIGINT COMPLIANCE REPORTING TEMPLATE.....	14
(U) APPENDIX E - NRO SIGINT COMPLIANCE INCIDENT REPORT FORM.....	15

(b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) NI 80-7-1 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, the NRO Business Function (NBF 80), and NRO Directive (ND) 80-7, this NRO Instruction (NI) sets forth the procedural implementation guidance and provides applicable information to perform the NRO Signals Intelligence (SIGINT) Compliance Incident Reporting process. All NRO personnel who perform tasks or have duties specific to SIGINT Incident Reporting will comply with this NI. When the work to be performed under an NRO contract must comply with this instruction, the program office shall list this instruction as a reference document in the contract statement of work.

(U) SECTION II - OVERSIGHT, SIGINT COMPLIANCE INCIDENT REPORTING

(U) The sub-sections that follow detail the SIGINT Compliance Incident Reporting.

(U) Governing NBF

(U) NBF-80, *Oversight*

(U) Description

(U//~~FOUO~~) NRO personnel provide support to the NRO [redacted] NRO-sponsored contractor facilities, and/or while co-located with other Intelligence Community (IC) elements. (b)(3)

(U//~~FOUO~~) This instruction provides the procedures for NRO personnel to accurately report unauthorized exposure of raw/unminimized, unprocessed SIGINT data as directed in Executive Order (E.O.) 12333, Department of Defense Regulation (DoDR) 5240.1-R, Presidential Policy Directive (PPD) 28 and NI 80-2-4, *Intelligence Oversight Reporting*.

(U//~~FOUO~~) For the purposes of this instruction an "incident" is defined as any activity that is believed to be unlawful or contrary to E.O., Presidential Directive, or Department of Defense (DoD) and NRO policies and regulations.

(U) Instruction Point of Contact

(U) Office of Policy and Strategy; Chief, [redacted] (b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) Support Systems

(U) NRO SIGINT Compliance training is available through the Office of Policy and Strategy (OP&S) [redacted] page. (b)(1)

(U) NRO [redacted] Web Page:
[redacted]
[redacted] (b)(3)

(U) Process Narrative

1.0 (U//~~FOUO~~) An individual recognizes a potential SIGINT Compliance reportable incident may have occurred. The initial recognition of a potential incident related to SIGINT Compliance can come about in a number of different ways.

1.1 (U//~~FOUO~~) The following is a sample of activities/events that are considered reportable:

1.1.1 (U//~~FOUO~~) Unauthorized access to raw SIGINT data (intentional or unintentional);

1.1.2 (U//~~FOUO~~) Access to data for which personnel are not cleared (Foreign Intelligence Surveillance Act (FISA));

1.1.3 (U//~~FOUO~~) Maintaining accesses after transferring to a new location or position (without re-justification);

1.1.4 (U) Password or account sharing;

1.1.5 (U) Unauthorized database access and/or queries;

1.1.6 (U//~~FOUO~~) Unauthorized retention of special authorization information (i.e., FISA) or raw SIGINT data;

1.1.7 (U) Tasking errors or de-tasking delays/errors;

1.1.8 (U) Unintentional collection; or

1.1.9 (U) Unauthorized dissemination of [redacted] (b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

2.0 (U//~~FOUO~~) The individual notifies their immediate supervisor, Program Manager (PM), Contract Officer Technical Representative (COTR) and/or sponsoring Directorate [redacted] if available, and submits an NRO SIGINT Compliance Incident Report. The individual may coordinate the report with the supervisor, PM, COTR, and/or [redacted] prior to submission. The report could come as notification from oversight and compliance personnel, from a self-reporting individual who is directly involved, or from automated reporting tools (i.e., [redacted])

(b)(3)

2.1 (U) A list of SIGINT [redacted] can be found on the NRO OP&S [redacted] web page under the Partners tab:

(b)(3)

2.2 (U//~~FOUO~~) The individual must complete the NRO SIGINT Compliance Incident Report Form using either the NRO SIGINT Compliance Incident Reporting Form found on the OP&S [redacted] web site or the [redacted] application.

(b)(3)

2.2.1 (U//~~FOUO~~) If using the NRO SIGINT Compliance Incident Report Form, complete the template in Appendix D and email it to [redacted] (includes the Intelligence Oversight Program Manager (IOPM) in the Office of the General Counsel (OGC), [redacted] and the [redacted]. The NRO template can also be found on the NRO OP&S [redacted] web page under the Standards tab:

(b)(3)

(b)(3)

2.2.2 (U//~~FOUO~~) Using the [redacted] (see Appendix E) automatically notifies the IOPM, [redacted] and [redacted]

(b)(3)

(b)(3)

2.3.1 (U//~~FOUO~~) Complete the [redacted]

(b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

2.3.2 (U//~~FOUO~~) Complete the NRO SIGINT Compliance Incident Report Form, and submit the report to the on-site NRO-facility leadership and the NRO-directorate leadership and email it to [REDACTED]

(b)(3)

2.3.3 (U//~~FOUO~~) If reporting through NSA channels [REDACTED]

(b)(3)

2.4 (U//~~FOUO~~) NRO-directorate leadership reviews the report and coordinates appropriate mitigating actions with the submitting unit, as needed.

3.0 (U) The [REDACTED] in coordination with the sponsoring Directorate [REDACTED] and Leadership, reviews and recommends appropriate actions which could include withdrawal of data accesses; purging of data; new or revised policies and/or procedures; requiring new or revised capabilities; additional training, and/or legal action if a violation of law has occurred. As needed and when appropriate, [REDACTED] will consult with the NRO IOPM, [REDACTED] and OGC and NSA when appropriate. Only the OGC can decree a violation of law.

(b)(3)

3.1 (U) Reported incidents that are determined to be in compliance will be annotated as such and closed by the [REDACTED]

(b)(3)

3.2 (U) [REDACTED] will engage with the reporting entities to investigate and provide guidance for closure.

(b)(3)

4.0 (U//~~FOUO~~) [REDACTED] will monitor incidents through closure and provide updated reports to the IOPM and reporting entities.

(b)(3)

4.1 (U) If the report is not already in [REDACTED] the [REDACTED] will enter the report into the [REDACTED]

(b)(3)

4.2 (U) [REDACTED] will ensure that all reports are updated.

(b)(3)

5.0 (U//~~FOUO~~) [REDACTED] will consolidate all reports and provide input to the OGC quarterly NRO Intelligence Oversight Report to the Department of Defense Senior Intelligence Oversight Official (DoD SIOO).

(b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) Process Flow Diagram

(U) Figure 1: NRO SIGINT Compliance Incident Reporting
Process

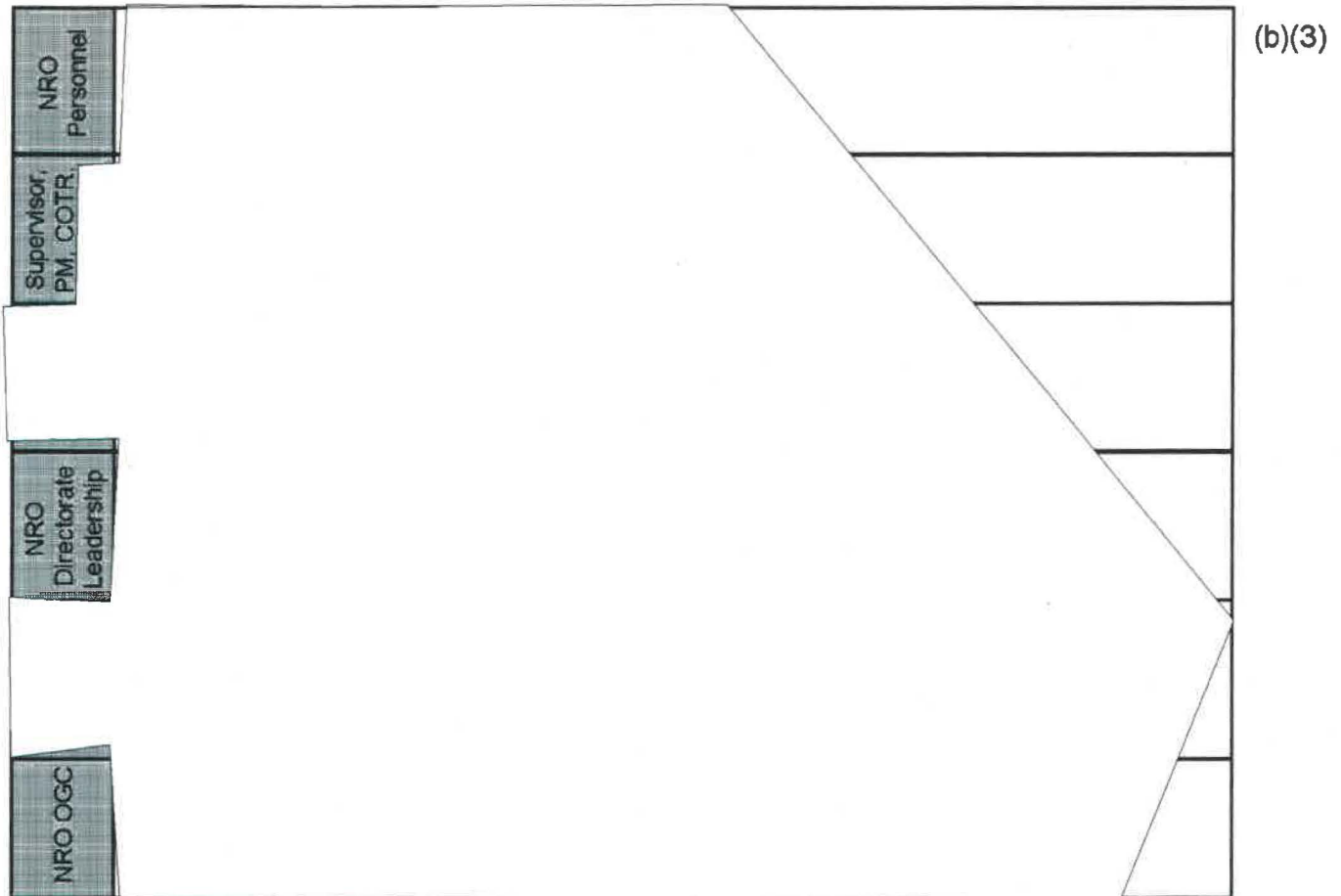


Figure is UNCLASSIFIED//~~FOUO~~

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
 FY 2015

(U) Table 1: Risk & Internal Control Table

Risk	Internal Control
(U) Not understanding the reporting process for the NRO/NSA could potentially delay the reporting of an incident.	(U) Provide up-to-date training and additional resources via the [redacted] web page. Keep Directorate and Office SIGINT [redacted] apprised of updates to ensure information is shared with NRO workforce.
(U) Delay in reporting an activity as soon as it is identified could cause unnecessary delays in ensuring [redacted] properly protected.	(U) Work with the Directorate and Office SIGINT [redacted] to ensure the workforce understands their reporting responsibilities within their respective chain of commands.

(b)(3)

(b)(3)

(b)(3)

Table is UNCLASSIFIED

(U) SECTION III - CONFIGURATION CONTROL

(U) All changes to this Oversight, Signals Intelligence Compliance Incident Reporting Instruction require NBF 80 owner approval in coordination with OP&S [redacted]

(b)(3)

(U) APPROVING SIGNATURE

(U) With the authority delegated by the NBF owner for Oversight, I confirm that this document provides a complete representation of the SIGINT Compliance Incident Reporting Instruction and that the document has been coordinated with stakeholders of the process.

June 26, 2015
 Date

(b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) APPENDIX A - PROCESS FLOW DIAGRAM LEGEND

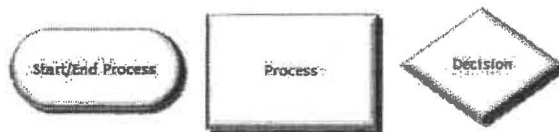


Figure is UNCLASSIFIED

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
 FY 2015

(U) APPENDIX B - ACRONYM LIST AND GLOSSARY

Term and Acronym	Definition
(U) Compliance	(U) Ensuring that SIGINT information is handled in a way that protects the rights of U.S. persons in a constitutionally acceptable way. Ensuring as well that Second Party person information will be handled in accordance with the applicable laws and regulations of [REDACTED] Compliance is applicable to all phases of the SIGINT process (tasking, collection, processing, exploitation, dissemination, and storage). This applies to the authorities delegated to the NRO by the Director, NSA (DIRNSA).
(U) DoD	(U) Department of Defense
(U) DoDR	(U) Department of Defense Regulation
(U) DoD SIOO	(U) Department of Defense Senior Intelligence Oversight Officer
(U) E.O.	(U) Executive Order
(U) Incident	(U) Activity that is believed to be unlawful or contrary to law, Executive Order, IC/DoD directives and regulations, or other relevant policies.
(U) IC	(U) Intelligence Community
(U) IOO	(U) Intelligence Oversight Officer
(U) IOPM	(U) Intelligence Oversight Program Manager
(U) NBF	(U) NRO Business Functions are functionally aligned and document the core business functions essential to successfully manage the NRO. An NBF defines the function, identifies its scope, and outlines senior-level roles and responsibilities
(U) ND	(U) NRO Directives are generated by the responsible NBF owner; establishes policy and direction for NBF execution.
(U) NI	(U) NRO Instructions are generated by the responsible NBF owner; provides detailed process steps from start to finish for a particular ND.
(U) NSA	(U) National Security Agency
(U) OGC	(U) Office of General Counsel
(U) OP&S	(U) Office of Policy and Strategy
(U) Oversight	(U) The process of ensuring that all intelligence- and counterintelligence-related activities are conducted in accordance with applicable laws, Executive Orders, directives, regulations, and policies. This applies to the authorities assigned to the NRO by executive order.
(U) PM	(U) Program Manager

(b)(3)

(b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
 FY 2015

Term and Acronym	Definition
(U) Questionable Activity	(U) Refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive Order, Presidential Directive, or DoD Policy.
(U) Raw SIGINT Data	(U// FOUO) Any SIGINT acquired either as a result of search and development, or targeted collection operations BEFORE the information has been evaluated for foreign intelligence AND minimization purposes.
(U) SIGINT	(U) Signals Intelligence
(U) Unminimized Data	(U// FOUO) Data has not been "minimized" to determine whether or not it contains U.S. persons information.
(U) U.S. person	(U) A U.S. citizen, an alien known by the intelligence agency considered a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments.
(U) Violation	(U) Unlawful activities that are unintentional, willful and intentional, or especially egregious (knowingly repeated, involving a large number of records, or taking place over a significant period of time).

(b)(3)

(b)(3)

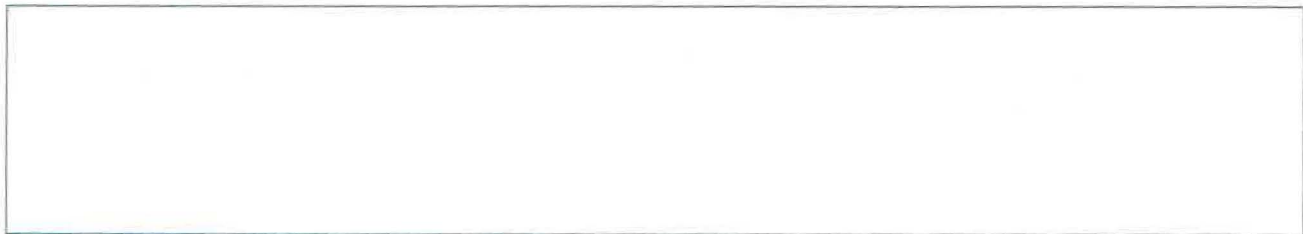
NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) APPENDIX C - REFERENCES/AUTHORITIES

a. (U) Executive Order 12333, *United States Intelligence Activities*, as amended.

b. (U) Department of Defense Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 December 1982.

c. (U) Presidential Policy Directive 28, *Signals Intelligence Activities*, 17 January 2014.



(b)(3)

e. (U) National Reconnaissance Office Governance Plan, 25 October 2011.

f. (U//~~FOUO~~) National Reconnaissance Office Business Function, 80, *Oversight*, 27 April 2012.

g. (U//~~FOUO~~) National Reconnaissance Office Directive 80-7, *Signals Intelligence Compliance*, 27 January 2014.

h. (U//~~FOUO~~) National Reconnaissance Office Instruction 80-2-4, *Intelligence Oversight Reporting*.

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015

(U) APPENDIX D - NRO SIGINT COMPLIANCE REPORTING TEMPLATE

(U//~~FOUO~~) NRO SIGINT Compliance Incident Report Format

(U//~~FOUO~~) (Site DDDMMYYY) SIGINT Compliance Incident Report

- a. **(Portion Mark) Title/Category:** (Note: Insert a "Title" or "Category" for the event being reported.)
- b. **(Portion Mark) Incident Description:** (Note: Provide a detailed description of the event. Include all relevant details. This entry is free flowing and may include multiple narrative paragraphs.)
- c. **(Portion Mark) Reason for Report:** (Note: Include the document cited as the basis of the report and a brief description to support the linkage to the document.)
- d. **(Portion Mark) Significance of the Event:** (Note: Provide your perspective of significance of the event. Was there potential for additional questionable activities? Was the event limited and highly unlikely to cause any harm to the NRO or violate additional tenants of the key documents?)
- e. **(Portion Mark) Event/Cause Analysis:** (Note: Include the results of any analysis of the event to support the cause, affect a solution, or otherwise, support the actions taken. This analysis may include situational, cause/effect, or trend analysis.)
- f. **(Portion Mark) Remedial Actions Taken:** (Note: Provide a description of actions taken, or planned, to correct the procedure or prevent the situation from reoccurring.)
- g. **(Portion Mark) Point of Contact:** (Note: Provide the name, phone number and email address of the individual who should be contacted if additional information or clarification is required.)
- h. **(Portion Mark) NSA Report Number:** (Note: If the event has been reported through NSA channels, include the report reference number for cross-reference purposes.)
- i. **(Portion Mark) Additional Comments:** (Note: Include any additional, relevant comments that may assist the NRO OGC, in understanding the event and actions taken or not taken.)

(b)(3)
(b)(3)

NI 80-7-1, Signals Intelligence Compliance Incident Reporting
FY 2015(U) APPENDIX E - NRO SIGINT COMPLIANCE INCIDENT
REPORT FORM

(b)(3)

(U//FOUO) NRO SIGINT Compliance Incident Report Format in

(b)(3)

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION: TOP SECRET//SI//TK//REL TO USA, FVEY

COMPLIANCE AUDITING & REPORTING

Incident Report

Point of Contact

*Name:	*Phone:
*Organization/Contractor:	*Email:
*Location:	

Incident Details

*Title/Category:	*Location of Incident:	*NSA Report Number:
------------------	------------------------	---------------------

*Incident Description:

*Significance of Event:

*Event Cause/Analysis:

*Remedial Actions Taken:

Additional Comments:

*Classification:

Incident Affected Sites:

*Check all affected sites(s) to be notified:

Additional Email Recipients:

I Certify that I have Portion-Marked this Form: ☐

Clear Cancel Submit

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION: TOP SECRET//SI//TK//REL TO USA, FVEY

(b)(3)

National Reconnaissance Office

Business Function 80, Oversight

Directive 80-7, Signals Intelligence Compliance

**Instruction 80-7-4, Signals Intelligence Compliance and
Data Protection Plans (C&DPP)**



3 AUGUST 2015

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
 FY 2015

TABLE OF CONTENTS

(U) NI 80-7-4 CHANGE LOG	3
(U) SECTION I - INTRODUCTION.....	4
(U) SECTION II - OVERSIGHT, SIGINT COMPLIANCE AND DATA PROTECTION PLANS.....	4
(U) Governing NBF.....	4
(U) Description.....	4
(U) Instruction Point of Contact.....	6
(U) Support Systems.....	6
(U) Process Narrative.....	6
(U) Process Flow Diagram.....	9
(U) Table 1: Risk & Internal Control Table.....	10
(U) SECTION III - CONFIGURATION CONTROL.....	10
(U) APPROVING SIGNATURE.....	10
(U) APPENDIX A - PROCESS FLOW DIAGRAM LEGEND.....	11
(U) APPENDIX B - ACRONYM LIST AND GLOSSARY.....	12
(U) APPENDIX C - REFERENCES/AUTHORITIES.....	14

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

(U) NI 80-7-4 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, the NRO Business Function (NBF) 80, and NRO Directive (ND) 80-7, this instruction sets forth the procedural implementation guidance and provides applicable information to perform the NRO Signals Intelligence (SIGINT) Compliance and Data Protection Plans (C&DPP) process. All NRO personnel who perform tasks or have duties specific to accessing and retaining raw SIGINT data will comply with this NRO Instruction (NI). When the work to be performed under NRO authorities and/or an NRO contract must comply with this instruction, the program office shall list this instruction as a reference document in the contract statement of work. Failure to comply with this instruction may result in loss of access to raw SIGINT data.

(U) SECTION II - OVERSIGHT, SIGINT COMPLIANCE AND DATA PROTECTION PLANS

(U) The sub-sections that follow detail the SIGINT Compliance and Data Protection Plans.

(U) Governing NBF

(U) NBF 80, Oversight

(U) Description

(U) This NI provides guidance on the drafting, submission and approval process for NRO SIGINT C&DPPs. In order to accomplish the NRO's research, development, testing and evaluation (RDT&E) and capability sustainment mission as detailed in Executive Order (E.O.) 12333, and as authorized in the National Security Agency (NSA)/NRO Data Sharing Memorandum of Understanding, the Office of Policy and Strategy [redacted] OP&S [redacted] has established the C&DPP process in order to maintain cognizance of NRO SIGINT-related activities, authorize, and to maintain strict access and control to raw and/or unminimized SIGINT data. All new contracts which require the handling of, or access to, raw SIGINT data acquired by NRO systems will have the necessary SIGINT compliance program requirements incorporated.

(b)(3)

(U) The three categories of C&DPPs described below are normally written by the prime contractor and routed through the appropriate Contracting Officer's Technical Representative

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

(COTR) and the Directorate or Office (D or O) [redacted] (b)(3)
[redacted] prior to submission to the [redacted] When no contracts
are involved, the government will write the appropriate C&DPP.

a. (U) Contract C&DPP - Establishes a record of delegated legal authority for NRO elements (Prime Contractor) to perform SIGINT specific RDT&E and capability sustainment functions authorized by E.O. 12333, Department of Defense Regulation 5240.1R and other appropriate documents. The Contract C&DPP is the foundational document in the NRO [redacted] C&DPP chain. The Contract C&DPP outlines the purpose and need for SIGINT data according to the contract requirements and identifies the policy for proper handling of the SIGINT data to be requested. (b)(3)

(U) Through the award of a contract, the U.S. government establishes a direct relationship with the prime. It is through the prime that authority and responsibilities are delegated to the sub-contractors to support the NRO SIGINT [redacted] (b)(3)
[redacted] Prime contracts shall
mandate all SIGINT compliance requirements to their subcontractors.

b. (U) Project C&DPP - is the most detailed, and comprehensive C&DPP in the process. This document outlines the data required to support the specific effort and serves as the record for approving data to be accessed and/or transferred in support of the task/project. This C&DPP bridges the authority to the task and defines the type of SIGINT data sets required to support the project. The key to this C&DPP is the level of detail contained in Section two of the Project C&DPP. In this section, the specific data requirements are identified, the contractor must identify why the SIGINT data access is required, and specify how the SIGINT data will be used. These requirements have a direct impact on the level of protection, access, training, and other policy matters.

c. (U) Facility C&DPP - The Facility C&DPP is required for any NRO government or contractor facility that receives or remotely accesses NRO acquired SIGINT data to support an NRO SIGINT effort. A Sensitive Compartmented Information Facility (SCIF) must be in place to receive or access SIGINT data. It is the responsibility of the SCIF accreditation holder (government or contractor) to prepare and submit the C&DPP. Once a facility has an approved Facility C&DPP, this C&DPP may be used as a reference for other NRO

**NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015**

Contract and Project C&DPPs, providing that security criteria and other provisions are met.

1. (U) Facilities may host the efforts and infrastructure for several tasks, projects, or contracts. The Facility C&DPP should be drafted and submitted to address the highest or most restrictive data-handling requirements for the different tasks, projects or contracts. When using [redacted]

(b)(3)

[redacted] to support an NRO SIGINT-related task, project, or contract, include the references to the associated agreements and/or SCIF accreditation as well as basic secure information technology infrastructure certification references that will be used to support that task, project, or contract.

2. (U) C&DPP templates are formatted to address all applicable SIGINT compliance directives and laws and should be used to expedite the review and approval process. It is the responsibility of the individual submitting the C&DPP to ensure that their C&DPP is properly classified and does not include any proprietary information. C&DPPs submitted into [redacted] may not contain Not Releasable to Foreign Nationals (NOFORN) information. If a Contract or Project C&DPP contains information NOFORN then a redacted Release to "Five Eyes" (REL FVEY) version of the C&DPP is entered into [redacted] and the NOFORN version of the C&DPP is submitted via email to OP&S [redacted]

(b)(3)

(U) Instruction Point of Contact

(U) Office of Policy and Strategy, Chief, [redacted]

(b)(3)

(U) Support Systems

(U) C&DPP templates and checklists are available through the OP&S [redacted]

(b)(3)

(U) The NRO [redacted] system provides a means for C&DPP submission: [redacted]

(b)(3)

(U) Process Narrative

1.0 (U) The process starts with the establishment of the authority for the work to be performed (Contract C&DPP), the

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

type of data required for performing the specified work (Project C&DPP), and the protection required of the data while in use and when being retained (Facility C&DPP).

2.0 (U//~~FOUO~~) It is the Prime Contractor's responsibility to initiate coordination and submission of the C&DPP in Microsoft (MS) Word format to [redacted]. This involves identifying a person within the company who has the authority to represent the company on C&DPP matters or delegating this authority. [redacted]

(b)(3)

(b)(3)

[redacted]
appropriate C&DPP. For the purposes of this instruction, "originator" will be used in describing the individual initiating this process.

2.1 (U) [redacted] hosts the workflow for recording approvals and serves as the historical repository for all C&DPPs. Along with uploading the record copy (MS Word version) of the C&DPP, the contractor must fill in the mandatory [redacted] data fields prior to submitting.

(b)(3)

2.2 (U) The originator must understand the exact type of C&DPP that is required, which will be dependent upon a number of factors:

2.2.1 (U) Existence of a Facility or Contract C&DPP;

2.2.2 (U) Addition of a new project being added to an existing Contract C&DPP; and

2.2.3 (U) Execution of a new contract.

2.3 (U) The originator must pre-coordinate the C&DPP with the respective COTR and the D or O [redacted] to ensure synchronization.

(b)(3)

3.0 (U) Once the C&DPP is drafted and has been pre-coordinated with the COTR and [redacted] it must be uploaded into [redacted] where it will be submitted for formal review. In accordance with the [redacted] workflow, the COTR and [redacted] will each review the C&DPP. The COTR and [redacted] will each [redacted]

(b)(3)

(b)(3)

[redacted] of the information contained within the C&DPP.

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

3.1 (U) If the COTR or [] non-concurs, the C&DPP will be sent back to the originator who will be responsible for addressing the identified issues. Once the issues have been addressed the C&DPP must be uploaded back into []

(b)(3)

3.2 (U) If the COTR or [] concurs, the [] workflow will send the C&DPP to OP&S [] for review.

(b)(3)

4.0 (U) OP&S [] will conduct a policy and technical compliance review which is followed by a legal review from a representative of the NRO Office of General Counsel (OGC). OP&S [] and OGC will conduct a review and either concur or non-concur based upon proper format and the sufficiency and appropriateness of the information contained within the C&DPP.

(b)(3)

(b)(3)

4.1 (U) If OP&S [] non-concurs, the C&DPP will be sent back to the originator who will be responsible for addressing the identified issues. The C&DPP will be uploaded back into [] by the originator once all items have been addressed and it will be routed back through the COTR and [] prior to OP&S [] second review.

(b)(3)

4.2 (U) OGC will conduct a legal review. OGC will conduct a review and either concur or non-concur based upon proper format and the sufficiency and appropriateness of the information contained within the C&DPP.

4.3 (U) If OGC non-concurs, the C&DPP will be sent back to OP&S [] who will coordinate with the originator and submit a revised version to OGC in order to minimize response time.

(b)(3)

(b)(3)

5.0 (U) After OP&S [] and OGC have concurred, the [] workflow will send the C&DPP to the SIGINT Compliance Officer (SCO) for final review and approval.

5.1 (U) If the SCO non-concurs, the C&DPP will be sent back to the originator for the issues to be addressed. These changes should be coordinated back through the applicable COTR and [] prior to the C&DPP being uploaded back into []

(b)(3)

5.2 (U) The SCO will conduct the final review and validation of the C&DPP. Once approved by the SCO, the process then allows for the identified personnel to access and retain SIGINT data for the purpose of conducting the NRO's [] in accordance with the C&DPP documentation.

(b)(3)

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

6.0 (U) After the C&DPP has been approved, minor updates to items such as internet protocol addresses, personnel, and Period of Performance changes can be coordinated and approved by the COTR. The updated version needs to be annotated and uploaded into enforces the appropriate approval chain of command.

(b)(3)

(U) Process Flow Diagram

(b)(3)

Figure is UNCLASSIFIED

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

(U) Table 1: Risk & Internal Control Table

Risk	Internal Control
(U) Failure to submit the appropriate C&DPP could result in a violation of contract deliverable.	(U) OP&S [] has implemented a proven process that includes the contractor program manager, COTR, and [] to ensure full awareness and compliance.
(U) Accessing SIGINT data without approved C&DPPs constitutes unauthorized access to SIGINT data.	(U) The C&DPP process establishes guidelines to ensure proper procedures are available and being followed to prevent unauthorized access.

Table is UNCLASSIFIED

(U) SECTION III - CONFIGURATION CONTROL

(U) All changes to this instruction require NBF owner approval in coordination with OP&S []

(U) APPROVING SIGNATURE

(U) With the authority delegated by the NBF owner for Oversight, I confirm that this document provides a complete representation of the SIGINT C&DPP instruction and that the document has been coordinated with stakeholders of the process.



SIGINT Compliance Officer, NRO

8/3/2015
Date

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

(U) APPENDIX A - PROCESS FLOW DIAGRAM LEGEND



Figure is UNCLASSIFIED

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
 FY 2015

(U) APPENDIX B - ACRONYM LIST AND GLOSSARY

Term and/or Acronym	Definition
(U) C&DPP	(U) Compliance and Data Protection Plan authorizes access to a specific set of NRO collected and stored data files to a specified person or group of people (named individually) for a specific purpose at a particular site.
(U) Contract C&DPP	(U) Contract C&DPP describes the task the contractor is to perform.
(U) COTR	(U) Contracting Officer Technical Representative
(U) D or O	(U) Directorate or Office
(U) E.O.	(U) Executive Order
(U) Facility C&DPP	(U) Facility C&DPP provides a description of the physical and system level protections in place to protect SIGINT data that will be accessed or used within a specific facility.
(U) Information Technology	(U) Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of the preceding sentence, equipment is used directly or is used by a contractor under a contract which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It is further delineated by Business Information Technology, Enterprise Information Technology, and Mission Information Technology.
(U) MS	(U) Microsoft
(U) NBF	(U) NRO Business Functions are functionally aligned and document the core business functions essential to successfully manage the NRO. An NBF defines the function, identifies its scope, and outlines senior level roles and responsibilities
(U) ND	(U) NRO Directives are generated by the responsible NBF owner; establishes policy and direction for NBF execution.
(U) NI	(U) NRO Instructions are generated by the responsible NBF owner; provides detailed process steps from start to finish for a particular ND.
(U) NOFORN	(U) Not Releasable to Foreign Nationals
(U) NSA	(U) National Security Agency
(U) OP&S	(U) Office of Policy and Strategy
(U) OGC	(U) Office of General Counsel

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
 FY 2015

Term and/or Acronym	Definition
(U) Project C&DPP	(U) Project Compliance and Data Protection Plan describes in specific terms information about the project and the data needed to perform the project.
(U) Raw SIGINT Data	(U// FOUO) Any SIGINT acquired either as a result of search and development, or targeted collection operations before the information has been evaluated for foreign intelligence and minimization purposes (unevaluated and unminimized).
(U) SIGINT	(U) Signals Intelligence
(U) SCIF	(U) Sensitive Compartmented Information Facility
(U) SCO	(U) SIGINT Compliance Officer
(U) SSP	(U) System Security Plan
(U) Sustainment	(U) To keep in existence; maintain, continue, prolong: <i>sustain an effort.</i>
(U) Unminimized Data	(U// FOUO) Data has not been "minimized" to determine whether or not it contains U.S. Persons information.
(U) U.S. Person	(U) A U.S. citizen, an alien known by the intelligence agency considered a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments.

(b)(3)

(b)(3)

(b)(3)

NI 80-7-4, Signals Intelligence Compliance and Data Protection Plans
FY 2015

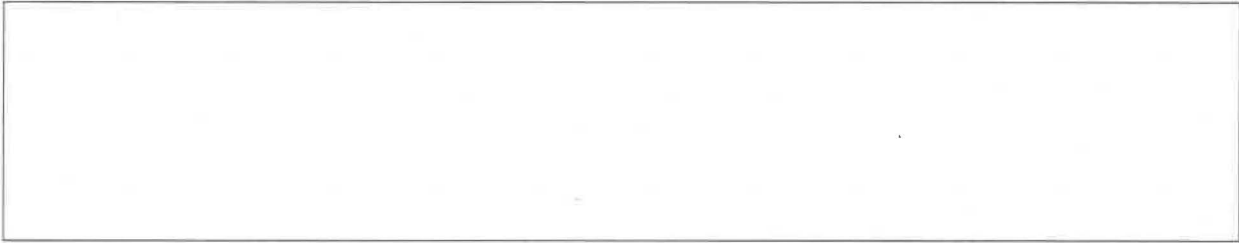
(U) APPENDIX C - REFERENCES/AUTHORITIES

a. (U) Executive Order 12333, *United States Intelligence Activities*, as amended.

b. (U) Department of Defense Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 December 1982.

c. (U) Presidential Policy Directive 28 (PPD-28), "Signals Intelligence Activities," January 17, 2014.

d. (U) Department of Defense Directive 5015.2, *DoD Records Management Program Directive*, dated 6 March 2000 and certified current as of 21 November 2003.



(b)(3)

f. (U) NRO Governance Plan, 25 October 2011.

g. (U//~~FOUO~~) NRO Business Function, 80, *Oversight*, 27 April 2012.

h. (U//~~FOUO~~) NRO Directive 80-7, *Signals Intelligence Compliance*, 27 January 2014.

i. (U) NRO Directive 56-1, *Records Management*, 12 March 2013.

National Reconnaissance Office
Business Function 80, Oversight
Directive 80-2, Office of General Counsel Framework
Instruction 80-2-4, Intelligence Oversight Reporting



4 SEPTEMBER 2015

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

TABLE OF CONTENTS

(U) NI 80-2-4 CHANGE LOG	3
(U) SECTION I - INTRODUCTION	4
(U) SECTION II - NBF 80 OVERSIGHT DOCUMENTATION	4
(U) Governing NBF	4
(U) Description	4
(U) Instruction Point of Contact	5
(U) Support Systems	5
(U) Process Narrative	5
(U) Process Flow Diagram	11
(U) Table I: Risk & Internal Control Table	12
(U) SECTION III - CONFIGURATION CONTROL	13
(U) APPROVING SIGNATURE	13
(U) APPENDIX A - PROCESS FLOW DIAGRAM LEGEND	14
(U) APPENDIX B - ACRONYM LIST AND GLOSSARY	15
(U) APPENDIX C - REFERENCES/AUTHORITIES	16

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

(U) NI 80-2-4 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks

**NI 80-2-4, Intelligence Oversight Reporting
FY 2015**

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, the NRO Business Function (NBF) 80, and NRO Directive (ND) 80-2, this NRO Instruction sets forth procedural implementation guidance and applicable information regarding the Intelligence Oversight (IO) Reporting process. Specifically, this NI details how to investigate and report in the event of an alleged IO incident at the NRO (i.e., a significant or highly sensitive matter involving an intelligence activity or intelligence personnel, or a questionable intelligence activity). All NRO personnel, including contractors, will comply with this NRO Instruction (NI). For all NRO contracts, the program office shall list this Instruction as a reference document in the contract statement of work.

(U) SECTION II - NBF 80 OVERSIGHT DOCUMENTATION

(U) The sub-sections that follow detail the IO Reporting process.

(U) Governing NBF

(U) NBF 80, Oversight

(U) Description

(U) Directive-Type Memorandum (DTM) 08-052, "DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters" implements Executive Branch guidance concerning the criteria and requirements for reporting IO matters and directs compliance with the stated guidance. Further, it establishes procedures to ensure complete and standardized reporting by the DoD Intelligence Components and other entities involved in intelligence activities, which include both foreign intelligence and counterintelligence activities. A significant or highly sensitive matter is a development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity (1) involving congressional inquiries or investigations; (2) that may result in adverse media coverage; (3) that may impact on foreign

**NI 80-2-4, Intelligence Oversight Reporting
FY 2015**

relations or foreign partners; and/or (4) related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method.

(U) A questionable intelligence activity is conduct during, or related to, an intelligence activity, as defined in Executive Order (E.O.) 12333, "United States Intelligence Activities," that may violate public law, Executive Order, Presidential Directive, or applicable DoD or NRO policy governing that activity.

(U) Executive Order 12333 stipulates that certain activities of intelligence components that affect United States (U.S.) Persons be governed by procedures issued by the agency head and approved by the Attorney General. For activities of Department of Defense (DoD) intelligence components that affect U.S. Persons, such procedures are set forth in DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons". It is applicable to all DoD intelligence components.

(U) Instruction Point of Contact

(U) IO Program Manager (IOPM)

(b)(3)

(U) Support Systems

NRO Management Information System (NMIS)

(U) Process Narrative

(U) The IO investigation and reporting procedures provided herein establish standardized guidance for all official NRO-sponsored military, government civilian, and contractor personnel. The following narratives explain the process flow for the IO program, and the investigating and reporting of IO incidents.

1.0 (U) IO Responsibilities

1.1 (U) The Office of General Counsel (OGC) is responsible for:

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

1.1.1 the sound and efficient management of IO by providing legal opinions and advice on questions of legality or propriety as appropriate;

1.1.2 ensuring the Director, National Reconnaissance Office is kept fully and currently informed of significant or highly sensitive matters involving an intelligence activity or intelligence personnel, and questionable intelligence activities;

1.1.3 determining whether intelligence activities are conducted in compliance with applicable law and regulations;

1.1.4 referring reports of suspected or confirmed IO incidents conducted by the NRO, or on behalf of the NRO, to either the Office of Policy & Strategy (OP&S) [redacted]

[redacted]

(b)(3)

1.1.5 hosting quarterly IO Officer (IOO) meetings.

1.2 (U) [redacted] is responsible for:

(b)(3)

[redacted]

(b)(3)

[redacted]

(b)(3)

[redacted]

(b)(3)

[redacted]

(b)(3)

[redacted]

(b)(3)

1.3 (U) IOOs are responsible for:

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

1.3.1 serving as custodian of all IO materials for their respective Directorate/Office, (D/O) maintaining current hardcopies of relevant documents (e.g., E.O. 12333, DoD 5240.1-R and DTM 08-052) and having them immediately available for any employee to copy or review;

1.3.2 providing copies of IO materials to D/O personnel;

1.3.3 providing assistance with the passing of any information regarding alleged IO incidents to the OGC IO team, [] or OP&S []

(b)(3)

1.3.4 attending quarterly IOO meetings hosted by the OGC IO Team;

1.3.5 assisting with raising awareness of mandatory training requirements, IO familiarization, and other IO activities; and

1.3.6 acting as the primary point of contact with the OGC IO Team or [] on all IO related matters.

(b)(3)

1.4 (U) The OP&S [] is responsible for:

(b)(3)

1.4.1 investigating reports of suspected or confirmed IO incidents that involve SIGINT;

1.4.2 verifying NRO personnel follow all applicable laws, orders, agreements, policies, and procedures related to use of SIGINT data by such personnel; and

1.4.3 identifying the rules, establishing standards, working with partners to monitor and identify risks and mitigate those risks, establishing training, and reporting the status of the NRO SIGINT Compliance Program to senior leadership.

1.5 (U) The OP&S [] is responsible for:

(b)(3)

1.5.1 investigating reports of suspected or confirmed IO incidents that involve DI;

1.5.2 managing domestic imagery use thru implementation of the NRO internal [] and the []

(b)(3)

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

[] processes contained in NRO Instruction 110-1-2, "Use of Domestic Imagery."

(b)(3)

2.0 (U) IO Reporting Process

(U) The following are the required process steps for reporting an alleged IO incident.

- a. (U) Initial notification;
- b. (U) Investigation; and
- c. (U) Reporting

2.1 (U) Initial Notification of Alleged IO Incident

2.1.1 (U) All NRO personnel will report alleged IO incidents immediately upon discovery through supervisory/command channels to either the [] or OGC. NRO personnel with concerns that their supervisory/command channel has not adequately addressed an alleged IO incident should seek out their IOO. Information about alleged IO incidents may also be sent directly to the [] or OGC from individuals internal or external to the NRO. [] or OGC will advise the appropriate IOO of any information received directly by the [] or OGC.

(b)(3)

2.1.2 (U) If an alleged IO incident involves SIGINT or DI, [] or OGC will notify either the OP&S [] or the OP&S [] about the incident. The OP&S [] or the OP&S [] will then investigate the alleged IO incident and provide a report on its recommended disposition to the [] and OGC.

(b)(3)

2.2 (U) Investigation of Alleged IO Incidents Involving SIGINT or DI by the []

(b)(3)

2.2.1 (U) After the OP&S [] receive notification of an alleged IO incident involving SIGINT or DI, they will have 30 calendar days to investigate the alleged IO incident and provide a report to the [] and OGC on the recommended disposition of the IO incident. Specifically, the report will contain the following:

(b)(3)

2.2.1.1 (U) Identification of the personnel committing the alleged IO incident by rank, civilian grade, or by name of the prime contractor; security clearance and access of the

**NI 80-2-4, Intelligence Oversight Reporting
FY 2015**

personnel involved; D/O of assignment, employment, attachment, or detail; and assigned duties at the time of the activity. Do not identify individuals by name or other personal identifier unless the or OGC so requests;

(b)(3)

2.2.1.2 (U) When and where the activity occurred;

2.2.1.3 (U) A description of the activity and how it constitutes an IO incident to include citation to the applicable portion(s) of DoD 5240.1-R, and other applicable law or policy as appropriate; and

2.2.1.4 (U) A description of the corrective actions planned or implemented.

2.3 (U) Investigation of Alleged IO Incidents

(b)(3)

(b)(3)

Specifically, the report will contain the following:

2.3.1.1 (U) Identification of the personnel committing the alleged IO incident by rank, civilian grade, or by name of the prime contractor; security clearance and access of the personnel involved; D/O of assignment, employment, attachment, or detail; and assigned duties at the time of the activity. Do not identify individuals by name or other personal identifier unless the OGC so requests;

2.3.1.2 (U) When and where the activity occurred;

2.3.1.3 (U) A description of the activity and how it constitutes an IO incident to include citation to the applicable portion(s) of DoD 5240.1-R, and other applicable law or policy as appropriate; and (4) A description of the corrective actions planned or implemented.

3.0 (U) IO Reporting Process for Ground Stations

3.1 (U) Each NRO Ground Station, under the authority of the NRO OGC and the established NRO IO Program, has appointed an NRO IOO responsible for IO and compliance at the site. As such,

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

any and all notifications of alleged IO incidents will follow the established investigation and reporting process set forth in this NI. While NRO Ground Stations have established internal operating instructions to provide site guidance on IO matters, that does not preclude NRO IOOs from fulfilling their obligation to report to the [] and OGC alleged IO incidents. As such, the NRO Ground Station IOOs shall work closely with multi-agency partner's IOOs when reporting IO incidents, as well as follow the established NRO IO program set forth above.

(b)(3)

4.0 (U) IO Reporting Process To DoD Senior IO Official (SIOO)

4.1 (U) After the [] or [] investigate and report on the alleged IO incident, the OGC will verify whether there is an IO incident that is reportable to the DoD SIOO. If there is a reportable IO incident, the OGC prepares a statement regarding the same to be included in the Quarterly IO Report to the DoD SIOO. If immediate referral is required, the OGC notifies the DoD SIOO immediately via secure means. In incidents where Congressional Notification (CN) is recommended, the IO Program Attorney will meet with the NRO GC and the Deputy Director, Office of Congressional and Public Affairs (DD/OCPA) to determine whether the incident rises to the level of a CN. If the incident rises to the level of a CN, the DD/OCPA will notify Congress via secure means while the IO Program Attorney notifies the DoD SIOO via secure means. Verbal reports should be documented with a written report as soon as possible thereafter.

(b)(3)

4.2 (U) OGC submits the Quarterly IO Report in the format prescribed by the DoD SIOO. Significant instances of fraud, waste, abuse, standards of conduct or ethics violations, financial misconduct, or conflicts of interest that affect intelligence operations do not need to be included in the Quarterly IO Report, but should be reported to NRO []

(b)(3)

4.2.2 (U) Quarterly IO reporting periods and report due dates are identified as follows:

<u>Quarter</u>	<u>Report Due to DoD SIOO</u>
First Quarter (JAN/FEB/MAR)	15 Apr
Second Quarter (APR/MAY/JUN)	15 Jul
Third Quarter (JUL/AUG/SEP)	15 Oct
Fourth Quarter (OCT/NOV/DEC)	15 Jan

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

(U) Process Flow Diagram

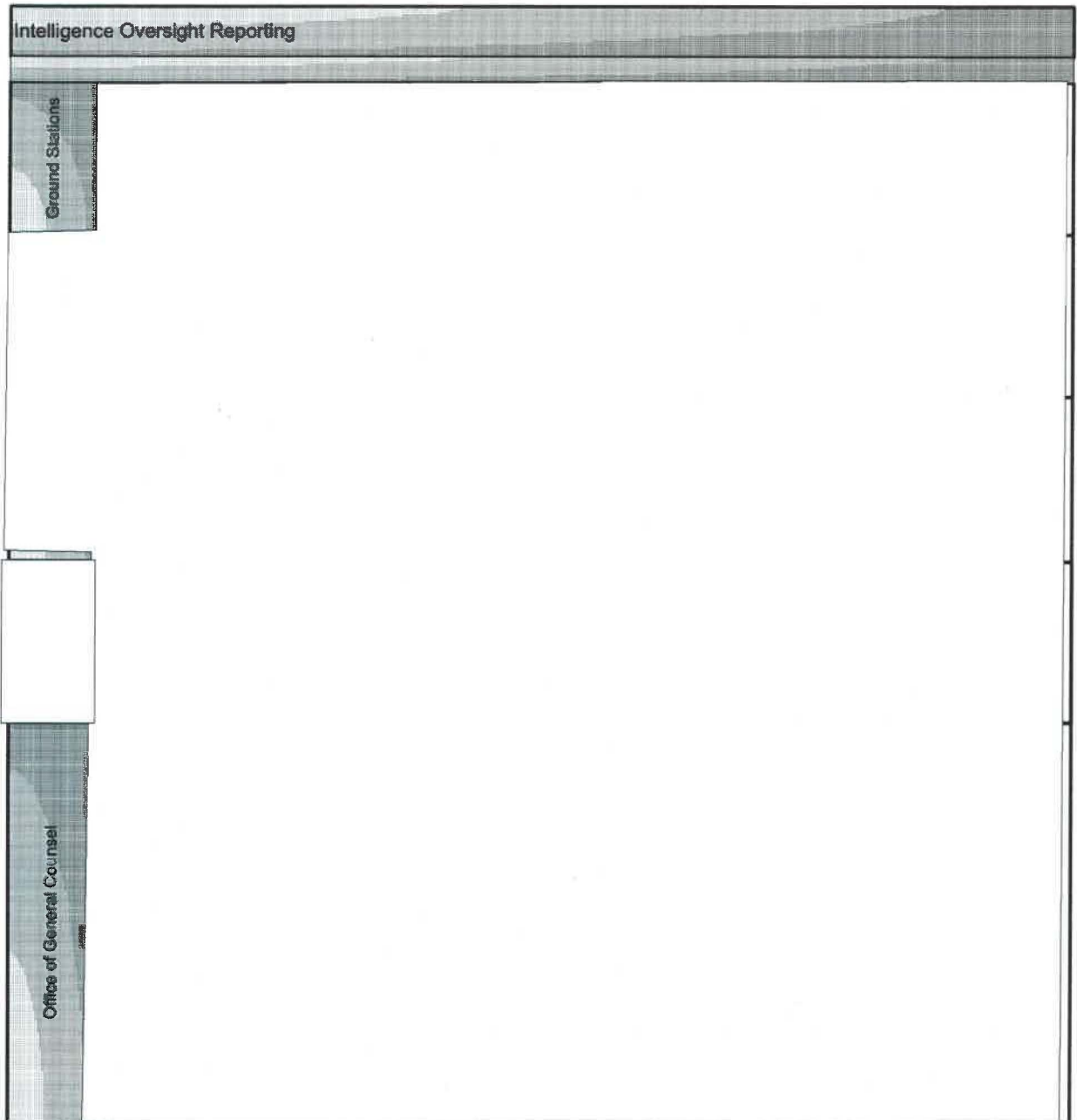


Figure is UNCLASSIFIED

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

(U) Table I: Risk & Internal Control Table

Risk	Internal Controls
(U) Inadequate reporting of questionable intelligence activities results in the failure to mitigate infringement upon the rights of U.S. Persons.	(U) OGC, OP&S [redacted] and [redacted] review initial incident, as applicable. (U) OGC, after the [redacted] [redacted] and report on the alleged IO incident, will verify whether there is a reportable IO incident to DoD SIOO. (U) GC and DD/OCPA determine if a potential IO violation should result in a CN.

(b)(3)

(b)(3)

Table is UNCLASSIFIED

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

(U) SECTION III - CONFIGURATION CONTROL

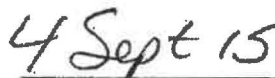
(U) All changes to the IO Reporting Instruction require GC approval.

(U) APPROVING SIGNATURE

(U) With the authority delegated by the NBF Owner for Oversight, I confirm that this document provides a complete representation of the Intelligence Oversight Reporting Instruction and that the document has been coordinated with stakeholders of the process.



Lisa T. Miller
General Counsel, NRO



Date

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

(U) APPENDIX B - ACRONYM LIST AND GLOSSARY

Term and Acronym	Definition
CN	Congressional Notification
DD/OCPA	Deputy Director, Office of Congressional and Public Affairs
DI	Domestic Imagery
D/O	Directorate/Office
DoD SIOO	Department of Defense Senior Intelligence Oversight Officer
DoD	Department of Defense
DTM	Directive-Type Memorandum
E.O.	Executive Order
GC	General Counsel
IO	Intelligence Oversight
IOO	Intelligence Oversight Officer
IOPM	Intelligence Oversight Program Manager
NBF	NRO Business Function
ND	NRO Directive
NI	NRO Instruction
NMIS	NRO Management Information System
NRO	National Reconnaissance Office
OGC	Office of General Counsel
OP&S	Office of Policy and Strategy
Questionable intelligence activity	A questionable intelligence activity is conduct during, or related to, an intelligence activity, as defined in Executive Order 12333, "United States Intelligence Activities," that may violate public law, Executive Order, Presidential Directive, or applicable DoD or NRO policy governing that activity.
SIGINT	Signals Intelligence
Significant or highly sensitive matter	A significant or highly sensitive matter is a development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity (1) involving congressional inquiries or investigations; (2) that may result in adverse media coverage; (3) that may impact on foreign relations or foreign partners; and/or (4) related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method.
U.S.	United States

(b)(3)

Table is UNCLASSIFIED

NI 80-2-4, Intelligence Oversight Reporting
FY 2015

(U) APPENDIX C - REFERENCES/AUTHORITIES

- a. (U) Executive Order 12333, as amended, 30 July 2008.
- b. (U) DoD 5240.1-R, Activities of Department of Defense (DOD) Intelligence Components that Affects U.S. Persons. 1982.
- c. (U) DTM 08-052, DOD Guidance for Reporting Questionable Intel Activities and Significant or Highly Sensitive Matters, July 2012, as amended.
- d. (U) NRO Business Function 80, Oversight, 4 April 2014.
- e. (U) NRO Directive 80-2, NRO Office of General Counsel Framework, 18 June 2013.

National Reconnaissance Office
Business Function 80, Oversight
Directive 80-2, NRO Office of General Counsel Framework



9 JUNE 2016

CL BY:
DECL ON: 25X1, 20660219
DRV FM: INCG 1.0, 13 February 2012

(b)(3)

ND 80-2, Office of General Counsel Framework
FY 2016

TABLE OF CONTENTS

(U) ND 80-2 CHANGE LOG	3
(U) SECTION I - INTRODUCTION.....	4
(U) SECTION II - APPLICATION.....	4
(U) SECTION III - REFERENCES/AUTHORITIES.....	4
(U) SECTION IV - POLICY.....	5
(U) SECTION V - ROLES AND RESPONSIBILITIES.....	6
(U) SECTION VI - DIRECTIVE POINT OF CONTACT.....	9
(U) SECTION VII - IMPLEMENTING INSTRUCTIONS.....	9
(U) APPROVING SIGNATURES.....	10
(U) APPENDIX - GLOSSARY AND ACRONYM LIST.....	11

ND 80-2, Office of General Counsel Framework
FY 2016

(U) ND 80-2 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks	
	18 June 2013			Initial Release	
1.0	9 June 2016		4 - 9	OGC is providing updates per NRO Governance Plan, NRO Instruction 20-4-1, Management Control Program/Statement of Assurance, and NRO Directive 20-5, NRO Governance	(b)(3)
2.0	24 October 2016		4 - 8	Administrative updates to incorporate Department of Defense Manual 5240.01 information	(b)(3)

ND 80-2, Office of General Counsel Framework
FY 2016

(U) SECTION I - INTRODUCTION

(U) In accordance with the National Reconnaissance Office (NRO) Governance Plan, this NRO Directive (ND) defines the scope, authorities, and responsibilities specific to NRO Business Function (NBF) 80, Oversight. The ND has been coordinated with appropriate stakeholders, and has been approved by the NBF owner, with administrative approval of the Director, Office of Policy and Strategy (OP&S). Official record copies are archived by OP&S.

(U) In accordance with the NRO Governance Plan, this ND implements specific provisions outlined in NBF 80.

(U) SECTION II - APPLICATION

(U) All NRO personnel who perform tasks or have duties specific to NBF 80 will comply with this ND and its corresponding instructions. When the work to be performed under an NRO contract must comply with this directive and corresponding instructions, the program office shall list these documents as reference documents in the contract statement of work.

(U) SECTION III - REFERENCES/AUTHORITIES

- a. (U) NRO Business Function 80, 4 April 2014.
- b. (U) Executive Order (E.O.) 12333, as amended, 30 July 2008.
- c. (U) Department of Defense (DoD) Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities, 2016.
- d. (U) DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 1982.
- e. (U) DoD Directive-Type Memorandum (DTM) 08-052, DoD Guidance for Reporting Questionable Intel Activities and Significant or Highly Sensitive Matters as amended, September 2015.
- f. (U) Title 28, United State Codes (U.S.C.), section 535, as amended.
- g. (U) Memorandum of Understanding: Reporting of Information Concerning Federal Crimes, August 1995, signed by the Attorney General; Secretary of Defense; Director of Central Intelligence; Director, National Security Agency; Director, Defense Intelligence

ND 80-2, Office of General Counsel Framework
FY 2016

Agency; Assistant Secretary of State, Intelligence and Research;
and the Director, Office of Non-Proliferation and National
Security, Department of Energy.

h. (U) Office of the Director of National Intelligence
Memorandum: Reporting Violations of Federal and State Criminal
Law, 3 July 2014.

[REDACTED] (b)(3)

j. ~~(S//REL)~~ Memorandum for General Counsel, NRO, [REDACTED]

[REDACTED] 3 January 2002.

(b)(1)
(b)(3)

k. ~~(U//FOUO)~~ Memorandum for General Counsel, NRO,
Appointment as Deputy Designated Agency Ethics Official,
17 November 2015.

l. ~~(U//FOUO)~~ Memorandum of Agreement between the Secretary of
Defense and the Director of National Intelligence concerning the
National Reconnaissance Office, 21 September 2010.

m. ~~(U//FOUO)~~ DoD Directive 5105.23, National Reconnaissance
Office, 28 June 2011, as amended 29 October 2015.

(U) SECTION IV - POLICY

~~(S//REL)~~ The General Counsel (GC) of the NRO shall be the
Chief Legal Officer of the NRO and shall be responsible for the
sound and efficient management of NRO legal affairs to include, but
not limited to, intelligence oversight (IO), ethics, crime
referrals, and [REDACTED]

[REDACTED] The NRO Office of
General Counsel (OGC), directed by the NRO GC, assists with
carrying out statutory and other responsibilities. OGC shall
provide legal advice and guidance to the Director, NRO (DNRO);
Principal Deputy Director, NRO; Deputy Director, NRO; and to all
personnel and entities of the NRO concerning matters within the
NRO's mission as set forth in References b., k., and l. above. All
members of the OGC shall report to the GC either directly, or
through the Principal Deputy GC (PDGC) or Deputy GC (DGC) who both
report to the GC. OGC shall provide legal advice through a
combination of centralized services and forward-deployed personnel.
The GC, PDGC, DGC, and the OGC Attorneys and Paralegal, acting on

(b)(1)
(b)(3)

ND 80-2, Office of General Counsel Framework
FY 2016

behalf of the GC, shall have access to any information the NRO GC deems to be necessary to implement the GC's statutory and other responsibilities.

(U) SECTION V - ROLES AND RESPONSIBILITIES

(U) The NRO GC has the exclusive authority and responsibility for:

a. (U) the provision of legal advice to the DNRO and all DNRO committees, boards, panels, and advisory groups;

b. (U) the conduct of all of the NRO's legal affairs;

c. (U) the authoritative and final legal interpretation within the NRO of any statute, regulation, E.O., or other provisions of law relating to NRO activities;

d. (U) the conduct of all liaison activities outside the NRO on legal matters, notwithstanding any other NRO governance document delineating liaison responsibilities;

e. (U) the adjustment, compromise, settlement, or denial of any administrative tort claim against the United States based upon the act or omission of any NRO employee;

f. (U) the protection or release of OGC information to the extent deemed appropriate by the GC and not precluded by law;

g. (U) the release, consistent with the DNRO authority, of NRO information to the courts, the Department of Justice, or otherwise in the conduct of the GC's statutory responsibilities, when the disclosure of that information is not precluded by law;

h. (U) the exercise of those authorities assigned to the GC via E.O. 12333, Memorandum of Understanding, and written delegation to the GC;

i. (U) the policy direction on all legal matters relating to the programs and operations of the NRO;

j. (U) the review of existing and proposed legislation and regulations relating to programs and operations of the NRO for legal sufficiency, and the making of recommendations concerning the impact of such legislation or regulations on the economy and

ND 80-2, Office of General Counsel Framework
FY 2016

efficiency in the administration of programs and operations administered or financed by the NRO or the prevention and detection of legal inefficiency in such programs and operations;

k. (U) the conduct, supervision, or coordination of relationships between the NRO and other federal organizations, state and local governmental agencies, and nongovernmental entities with respect to programs and operations administered or financed by the NRO when such matters relate to: (1) the promotion of economy and efficiency in the administration of such programs and operations administered or (2) the prevention of and detection of legal inefficiency in such programs and operations, or the identification of participants in such inefficient activities;

l. (U) the notifications to keep the DNRO, Congress, and the DoD Senior Intelligence Oversight Officer fully and currently informed, by means of the reports required concerning other serious problems, abuses, and deficiencies relating to the administration of programs and operations administered or financed by the NRO; recommending corrective action concerning such problems, abuses, and deficiencies; and reporting on the progress made in implementing such corrective action;

m. ~~(S//REL)~~ the submissions of a semi-annual report of all exports authorized pursuant to [redacted] (b)(1)
authority and all classified licenses sought in accordance with [redacted] (b)(3)

n. (U) the administration of the NRO ethics program as the NRO's Deputy Designated Agency Ethics Official;

o. (U) the administration of the Crimes Reporting program, in conjunction with the Office of Security and Counterintelligence;

p. (U) the assurance that all programs and operations of the NRO comply with applicable law and regulations [redacted] (b)(3)

q. (U) the expeditious notification to the Attorney General whenever the GC has reasonable grounds to believe there has been a violation of federal criminal law;

r. (U) the delegation of authority to the PDGC and DGC as appropriate and in accordance with NRO policies and procedures; and

ND 80-2, Office of General Counsel Framework
FY 2016

s. (U) the performance of such functions as the DNRO may prescribe.

(U) Under this Directive, NRO personnel shall:

a. (U//~~FOUO~~) familiarize themselves with NBF 80, E.O. 12333, DoD Manual 5240.01, DoD 5240.1-R, and DTM 08-052;

b. (U//~~FOUO~~) report to their local IO Officers (IOO), [redacted], OP&S, [redacted] and OGC any questionable NRO intelligence activity that may violate the law or the requirements of DoD Manual 5240.01 and DoD 5240.1-R; (b)(3)

c. (U//~~FOUO~~) if at NRO ground stations, report to their site Commander or Chief of Facility, their site National Geospatial-Intelligence Agency, NRO, or National Security Agency IOOs any questionable activities involving U.S. Person information;

d. (U//~~FOUO~~) know that those reporting such conduct as defined in this section are protected from retribution (DoD 5240.1-R, Chapter 14);

e. (U//~~FOUO~~) report to the GC any possible violation of state or federal criminal laws learned in the course of their official duties (E.O. 12333, Section 1.6(b); DoD Manual 5240.01, DoD 5240.1-R, C12.2.2 and 15.3.3.3; and 28 U.S.C. 535);

f. (U//~~FOUO~~) report "any significant or highly sensitive" intelligence matters to the GC (DTM 08-052);

g. (U//~~FOUO~~) complete annual ethics training;

h. (U//~~FOUO~~) complete annual E.O. 12333 training, including specific [redacted] if they are a United States (U.S.) government employee, U.S. military personnel, or contractor with access to an NRO Management Information System. This training is required irrespective of duty location of said NRO personnel; and (b)(3)

i. (U//~~FOUO~~) complete initial IO training and annual refresher training on [redacted] if they are involved in any planned efforts to perform, continue to perform or change [redacted] (b)(3)

ND 80-2, Office of General Counsel Framework
FY 2016

(U) SECTION VI - DIRECTIVE POINT OF CONTACT

(U) GC, NRO at

(b)(3)

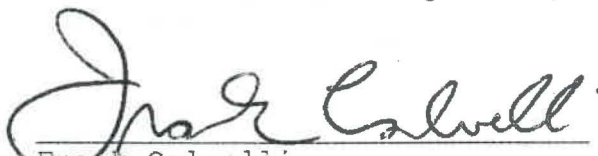
(U) SECTION VII - IMPLEMENTING INSTRUCTIONS

(U) The GC will approve and sign any implementing Instructions developed under NRO Directive 80-2.

ND 80-2, Office of General Counsel Framework
FY 2016

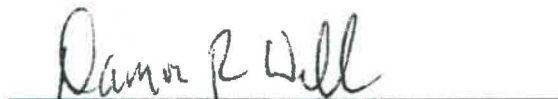
(U) APPROVING SIGNATURES

(U) As the NBF owner for NBF 80, Oversight, I confirm that this document provides a complete representation of the ND 80-2, NRO OGC Framework and the document has been coordinated with stakeholders in this process.



Frank Calvelli
Oversight NBF Owner

6/8/16
Date



Damon R. Wells
Director, Office of Policy
and Strategy

6/9/16
Date

ND 80-2, Office of General Counsel Framework
 FY 2016

(U) APPENDIX - GLOSSARY AND ACRONYM LIST

Term and Acronym	Definition
[REDACTED]	
DGC	Deputy General Counsel
DNRO	Director National Reconnaissance Office
DoD	Department of Defense
DTM	Directive Type Memorandum
E.O.	Executive Order
GC	General Counsel
IO	Intelligence Oversight
IOO	Intelligence Oversight Officer
[REDACTED]	
NBF	NRO Business Function
ND	NRO Directive
NRO	National Reconnaissance Office
NRO Personnel	NRO personnel encompasses all military, civilian, and contractor personnel assigned to, or supporting, NRO programs
OGC	Office of General Counsel
OP&S	Office of Policy and Strategy
PDGC	Principal Deputy General Counsel
SIGINT	Signals Intelligence
U.S. Person	United States Person
U.S.C.	United States Code

(b)(3)

(b)(3)

Chart is UNCLASSIFIED

NATIONAL RECONNAISSANCE OFFICE

Intelligence Oversight Training: Legal Limitations on



Activities

NRO Office of General Counsel
February 2017

(b)(3)





Training Objectives

Upon successful completion of this module, participants will be able to describe –

(b)(3)

-
- + (2) the reasons why such restrictions exist, given the constitutional, statutory, regulatory, and other authorities restricting the collection of data
 - + (3) the process for obtaining official approval to perform such activities.

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

2.



Objective (1)

What are the differences between

(b)(3)

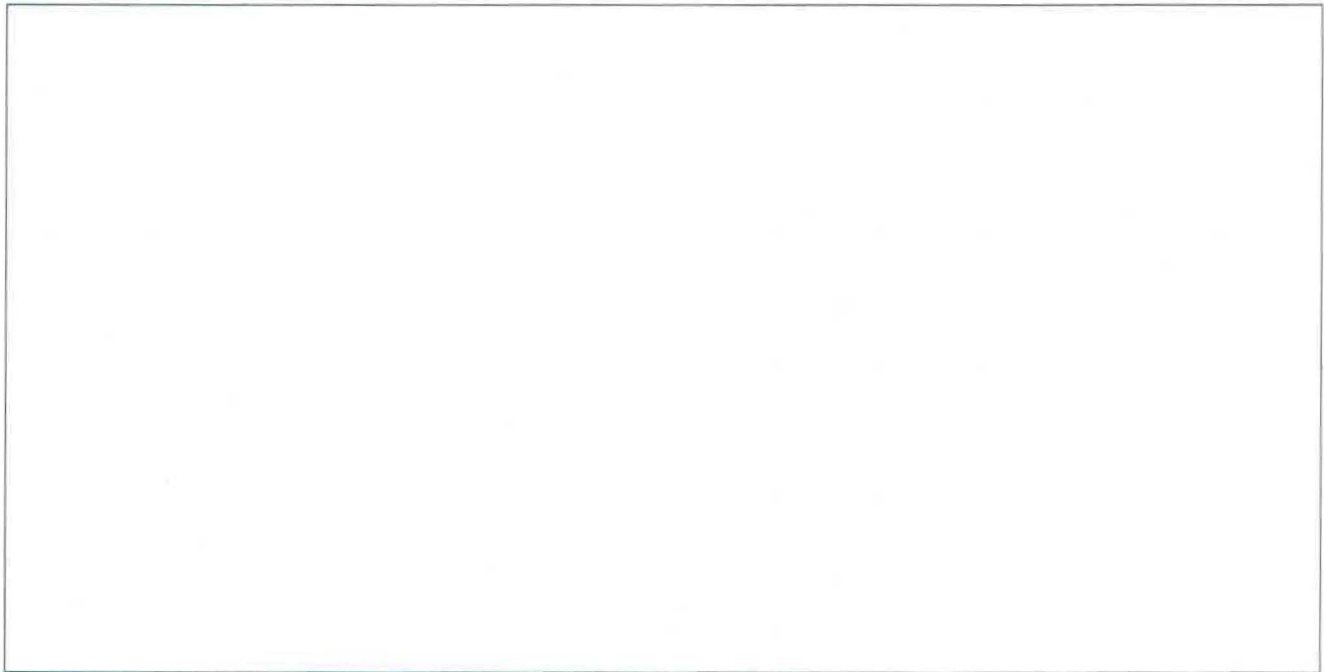
OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

3



(b)(3)



(b)(3)

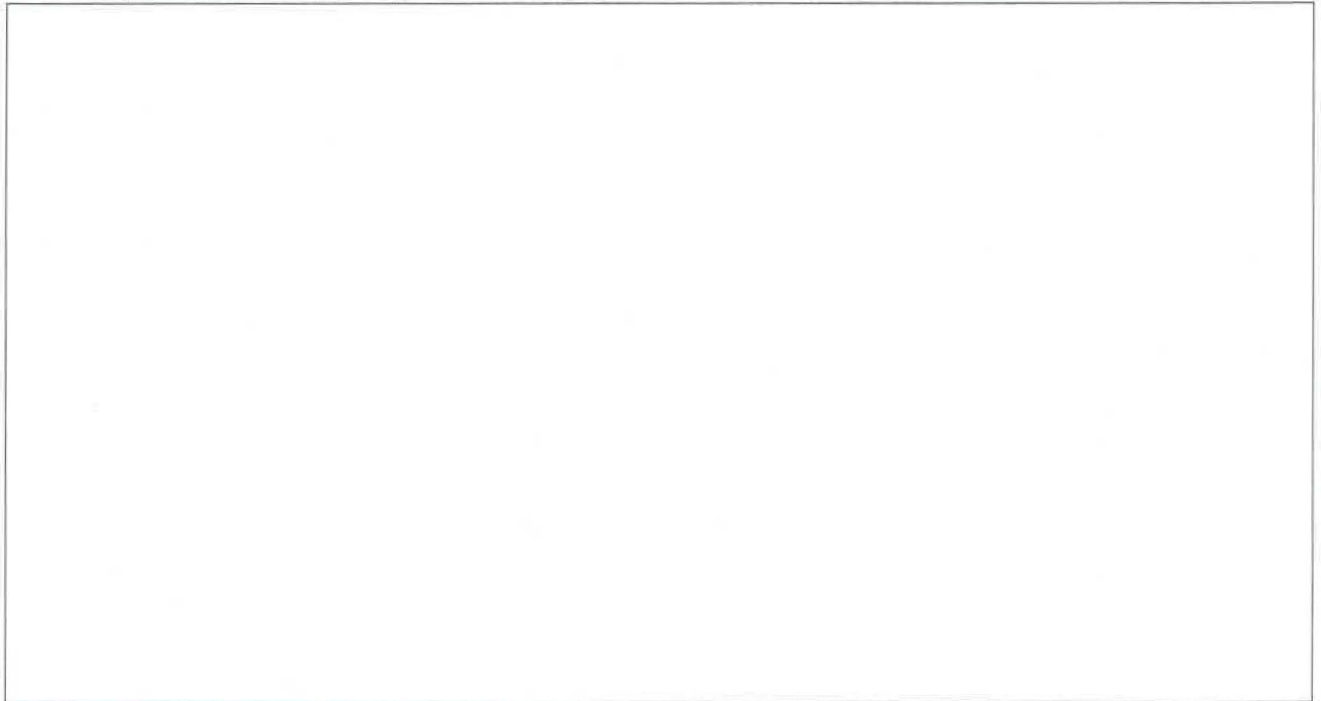
OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

4



(b)(3)



(b)(3)

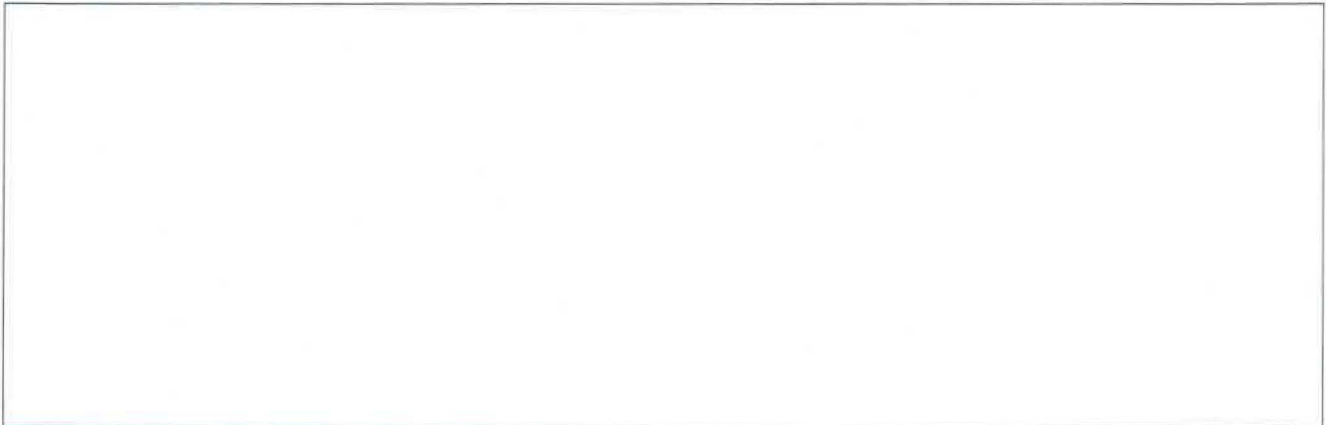
OFFICE OF GENERAL COUNSEL

~~UNCLASSIFIED (7) FOR OFFICIAL USE ONLY~~

5




(b)(3)




(b)(3)

+ Official approval is required 

(b)(3)

+ Questionable  activities must be reported

(b)(3)

+ Intelligence Oversight (IO) ensures that the conduct of intelligence *activities* conforms with US law and regulation, in particular protects legal rights/civil liberties of U.S. persons 

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

6



Review

+ Answer True or False to the following statements:

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

7



Objective (2)

How do the U.S. Constitution,
legislation, regulations, and
other authorities
restrict the **collection, dissemination,
and retention of data**, and
why do such restrictions exist?

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

8



US Person Information (USPI)

- + US person names
- + US person phone numbers
- + US person e-mails
- + US companies

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED / FOR OFFICIAL USE ONLY

9



How broad is US Person information or data?

+ Applies to:

(b)(3)

+ U.S. states and territories:

- + 50 States, District of Columbia, Puerto Rico, Guam, American Samoa, US Virgin Islands, Northern Mariana Islands, US territorial waters and airspace above such areas (See 50 U.S.C. 1801 (i), (j) and (o); and the UNCLOS III)

+ Other:

PPD-28 states **all persons**, regardless of nationality or where they reside, have legitimate privacy interests in the handling of their personal information; therefore, signals intelligence activities must include appropriate safeguards for **all PII**.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

10

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

11



Constitutional Authorities

Constitution of the United States of America, Bill of Rights

- + Freedom of speech (1st Amendment)
- + The right to be secure against “unreasonable searches and seizures” (4th Amendment)
 - + The 4th Amendment protects US citizens from unauthorized “search and seizure.”
 - + “US Persons” (certain individuals and entities in addition to US citizens) receive the same rights and protection as US citizens.
 - + Unauthorized interception of US Person private communications is **not** allowed.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

12.



Statutory Authorities

- + Electronic Communications Privacy Act (18 U.S.C. § 2510 *et seq.*)
 - + Prohibits unauthorized interception of wire, oral or electronic communications unless for law enforcement.
- + Stored Communications Act (18 U.S.C. § 2701 *et seq.*)
 - + Prohibits unauthorized intentional access of a facility through which electronic communication service is provided.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

13



Statutory Authorities – Cont'd

- + Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 *et seq.*) ("FISA")
 - + Permits the President, with Attorney General certification, to acquire foreign intelligence information using electronic surveillance without a court order.
 - + Requires minimizing the acquisition, retention and dissemination of information not available to the public concerning non-consenting US persons.
 - + Otherwise, a warrant is required.
 - + FISA court reviews requests for a warrant.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

14



Regulatory Authorities

- + DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities"
- + DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons"



(b)(1)

- + E.O. 12333

**OFFICE OF GENERAL COUNSEL**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

15

Unclassified



What is "collection" of US Person Information (USPI)?

- + DoDM 5240.01, Procedure 2 (§ 3.2)
- + Definition of "collection" (DoDM 5240.01 Glossary)

Information is collected when it is received by a Defense IC whether or not it is retained by the Component for intelligence or other purposes.
- + "Collected information" does not include:
 - + Information that only momentarily passes through a computer system of the Component;
 - + Information on the internet or in an electronic forum or repository outside the Component simply viewed or accessed but not copied, saved, supplemented or used in some manner;
 - + Information disseminated by other IC elements;
 - + Information maintained on behalf of another USG agency to which the Component does not have access for intelligence purposes.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

16



What is "retention" of USPI?

- + DoDM 5240.01, Procedure 3 (§ 3.3)
- + Definition of "retention" (DoDM 5240.01 Glossary)

The maintenance of information in either hard copy or electronic format regardless of how the information was collected or how it was disseminated to a Defense IC by another Component or element of the Intelligence Community.
- + Retention duration depends on whether collection was intentional, incidental, voluntarily provided, or fell into a "special circumstances" category.
 - + "Extended retention" and "permanent retention" require specific findings the information is reasonably believed to be necessary for the performance of an authorized intelligence mission.
- + Detailed Protections for USPI require USG evaluate and mark the information

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

17



What is "dissemination" of USPI?

- + DoDM 5240.01, Procedure 4 (§ 3.4)
- + Definition of "dissemination" (DoDM 5240.01 Glossary)

The transmission, communication, sharing, or passing of information outside a Defense IC by any means, including oral, electronic, or physical means. Dissemination includes providing any access to information in a Component's custody to persons outside the Component.
- + Information may be disseminated only if it was properly collected or retained.
- + Applies to USPI in any form.
- + Does not apply to the dissemination of information collected solely for administrative purposes or disseminated pursuant to other procedures approved by the Attorney General or court order.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

18



(b)(3)



(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

19



Executive Order (EO) 12333

- + The USG is obligated to protect the legal rights of all US Persons
 - + Legal rights include, but are not limited to, privacy and civil liberties (Sec. 1.1(b))
- + "US Person" means, under section 3.5(k):
 - + US citizen
 - + Permanent resident alien
 - + Unincorporated association substantially composed of US citizens or permanent resident aliens
 - + Any entity incorporated in the US not directed or controlled by a foreign Government

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

20



EO 12333 – Cont'd

- + Under section 2.3, IC elements may only collect, retain or disseminate information concerning US Persons if (among other reasons):
 - + the information is publicly available or collected with the consent of the person concerned
 - + the information constitutes foreign intelligence and is not collected for the purpose of acquiring information about the domestic activities of US Persons
 - + the information has been acquired by overhead reconnaissance and is not directed at specific US Persons

NOTE: Information inadvertently collected on US Persons is subject to retention and reporting rules.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

21



EO 12333 – Cont'd

+



limited to NRO's specified mission:

(b)(3)

"The Director of the NRO shall:

Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs..."

(Sec 1.7(d))

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

22.



EO 12333 – Cont'd

- + NRO's authority to collect data is limited to:
 - + NRO's specified mission (Sec 1.7);
 - + The tasking by another IC element in accordance with its official authority (Sec 1.7); or
 - + Assisting law enforcement agencies within the scope of their jurisdiction (Sec 2.6).

NRO does not produce intelligence.

OFFICE OF GENERAL COUNSEL

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

23



EO 12333 – Cont'd

+ NRO Authorities v. Other IC Authorities

+ NSA (Sec 1.7(c)):

- + “Collect (including through clandestine means), process, analyze, produce and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions”

+ CIA (Sec 1.7(a)):

- + “Collect (including through clandestine means), analyze, produce and disseminate foreign intelligence and counterintelligence”

+ The Intelligence and Counterintelligence elements of the Army, Navy, Air Force, and Marine Corps (Sec 1.7(f)):

- + “Collect (including through clandestine means), produce, analyze and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements.”

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

24



EO 12333 – Cont'd

- + NRO Authorities v. Authorities of other IC Elements –
 - + Intelligence Elements of the FBI (Sec 1.7(g)):

"Collect (including through clandestine means), analyze, produce and disseminate foreign intelligence and counterintelligence to support national and departmental missions in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director of the [FBI]."

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED - FOR OFFICIAL USE ONLY

25



EO 12333 Implemented by DoDM 5240.01

- + Pertinent chapters of DoDM 5240.01:
 - + Collection, retention and dissemination of USPI (Procedures 2 thru 4)
 - + Electronic surveillance (Procedure 5)
 - + Concealed Monitoring (Procedure 6)
 - + Undisclosed participation in Organizations (Procedure 10)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

20



Unintentional Collection of US Person Data

- + If US Person data is unintentionally collected during an authorized mission, you must immediately report the incident to:
 - + IO Officer (IOO) within your organization;
 - + OGC Program Attorney for IO*;
 - + OGC Program Attorney for your D/O;
 - + Your D/O Director of Security; and
 - + Your Contracting Officer and Contracting Officer Technical Representative (if violation relates to a contract).

* Call and ask to speak with the IO Program Attorney.

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

27



Consequences of failing to protect US Person information or data

+ Criminal and civil penalties:

+ FISA

Criminal – Up to \$10,000 fine / Up to 5 years in prison

Civil – Actual and punitive damages / litigation costs

+ Stored Communications Act

Criminal – Same as FISA for 1st offense; Up to 10 years in prison for 2nd offense

Civil – Same as FISA

+ Electronic Communications Privacy Act –

Up to \$10,000 civil fine / Up to 5 years in prison

+ Possible administrative discipline for the personnel who collected the data

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

28



Review

1. May NRO collect information on US Persons and their activities within the United States?
2.
3. Does NRO have the authority to collect data on behalf of another IC element?
4. Is NRO allowed to intercept private communications of US Persons without prior authorization?
5. What happens if NRO inadvertently collects US Person information during an authorized mission?
6. What categories of information are considered protected from collection on US Persons?

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

29



Objective (3)

What is the **process** for obtaining official approval on behalf of the NRO?

(b)(3)

**OFFICE OF GENERAL COUNSEL**

UNCLASSIFIED // FOR OFFICIAL USE ONLY

30



Step 1: Complete required training.

Take required [redacted] training and ensure
all associated [redacted] performers obtain
such training [redacted]

(b)(1)

(b)(1)

(b)(1)

(b)(1)

- + Initial training; and
- + Annual refresher training
- + (2) Office of Security and Counterintelligence (OS&CI)
online training thru NRO University (NROU)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

31



Step 2: Prepare
Request Package.

- + Impacts to the source and recipient of info/matter to be acquired if information or fact of collection is disclosed
- + Name and contract number of any affected contracts

OFFICE OF GENERAL COUNSEL

~~UNCLASSIFIED - FOR OFFICIAL USE ONLY~~

32



(b)

Request Package – Cont'd

- + Estimated cost
- + Availability of funding
- + Other resources needed or required
- + Program security risk
- + Alternative means of obtaining desired info or other matter



(b)

- + Apparent risks; or
- + Alternate means available

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

33



Step 3:

(b)(3)

+ Users must submit a request package for official review and approval for –

+ Proposed activity

(b)(3)

+ Changes in scope to previously approved activities

(b)(3)

+

(b)(3)

OFFICE OF GENERAL COUNSEL

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

34



(b)



(b)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

35



(b)(3)



(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED / FOR OFFICIAL USE ONLY

36



(b)(3)



(b)(3)

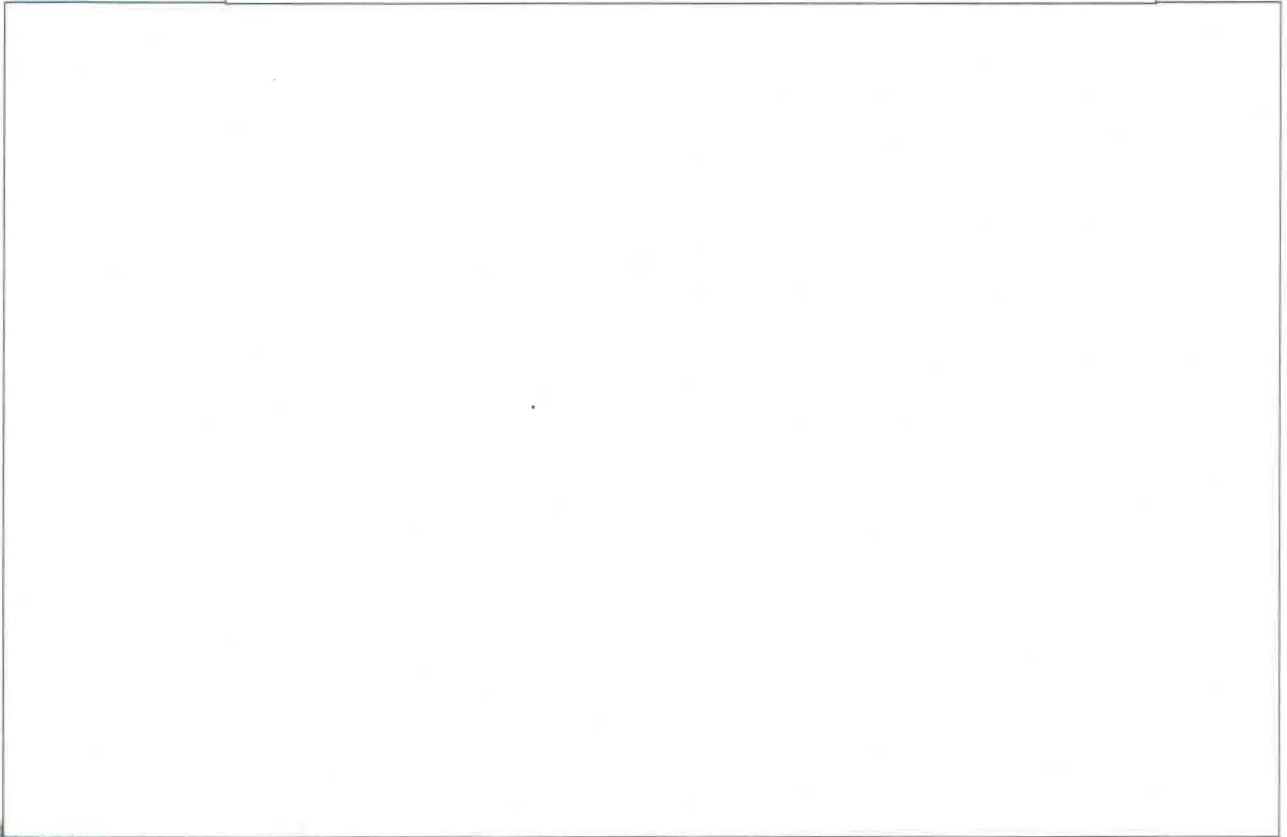
OFFICE OF GENERAL COUNSEL

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

37



(b)(3)



(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

38



Review

1.

2.

(b)(3)

3. Of the following items, which ones should be included with the Request Package?

a. Names, agencies, and other information regarding entities

(b)(3)

b. Estimated cost.

c. Program security risk.

d. Availability of funding.

e. All of the above.

f. None of the above.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED - FOR OFFICIAL USE ONLY

39



Knowledge Assessment (1)

[Empty rectangular box for knowledge assessment content]

(b)(1)

OFFICE OF GENERAL COUNSEL

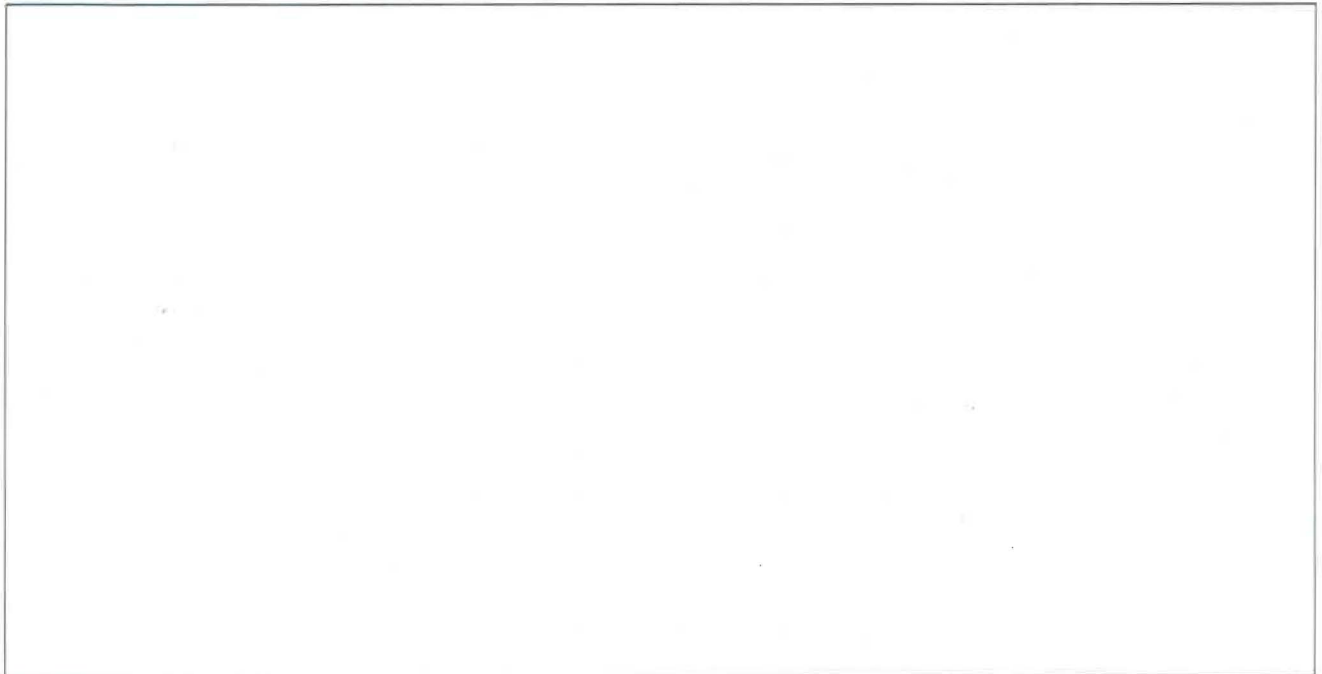
UNCLASSIFIED // FOR OFFICIAL USE ONLY

40



Knowledge Assessment – Cont'd (2)

(b)(3)



OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

41



Knowledge Assessment – Cont'd (3)

True or false?

NRO-applicable regulatory authorities restricting the collection, dissemination, and retention of data are –

- DoD Manual 5240.01, and

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

42.



Knowledge Assessment – Cont'd (4)

Why are there restrictions on collecting U.S. Persons' Information?

1. Constitutional protections for freedom of speech (1st Amendment).
2. Constitutional protections against unreasonable search and seizure (4th Amendment).
3. Electronic Communications Privacy Act prohibits unauthorized interception of wire, oral or electronic communications unless for law enforcement.
4. Stored Communications Act protects against intrusion into stored electronic data.
5. FISA minimizes the collection of information not publicly available without the consent of U.S. persons.
6. Executive Order 12333 protects the privacy and civil liberties of U.S. Persons.
7. All of the above.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

43



Knowledge Assessment – Cont'd (5)

When can the NRO collect information on U.S. Persons?

1. Any time a satellite system is threatened.
2. When directed to do so by county law enforcement.
3. When requested by the President of the United States.
4. When requested to do so by the CIA within CIA's authorities.
5. When a full moon occurs on a Thursday.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

44



Knowledge Assessment – Cont'd (6)

What action must you take if you unintentionally collect U.S. Person data during an authorized mission?

1. No action necessary.
2. Report the incident to your immediate supervisor.
3. Immediately report the incident to: the IO Officer, the IO Program Attorney, the attorney for your D/O, your Director of Security, and your contracting officer (if violation relates to a contract).
4. Report the incident to the DNRO and the SecDef.
5. Notify The Washington Post.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

45



Knowledge Assessment – Cont'd (7)

What information is captured by the requirement to protect "US Person information or data"?

1. Names and phone numbers of individuals residing in the 48 contiguous United States.
2. E-mail addresses of individuals residing in all 50 U.S. States.
3. Names and phone numbers of companies in all 50 States and U.S. territories.
4. Names, phone numbers, and e-mail addresses for individuals and companies located in: the U.S. 50 States and territories.

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

46



Knowledge Assessment – Cont'd (8)

True or False?

Failing to protect US Person information or data may result in criminal, civil, and administrative penalties.

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

47



Knowledge Assessment – Cont'd (9)

Provide a brief explanation regarding these acronyms.

1) NRO –

2)

3)

(b)(3)

OFFICE OF GENERAL COUNSEL

UNCLASSIFIED//FOR OFFICIAL USE ONLY

48



Knowledge Assessment – Cont'd (10)

What other training must you take to meet all of the training requirements for on behalf of NRO?

(b)(3)

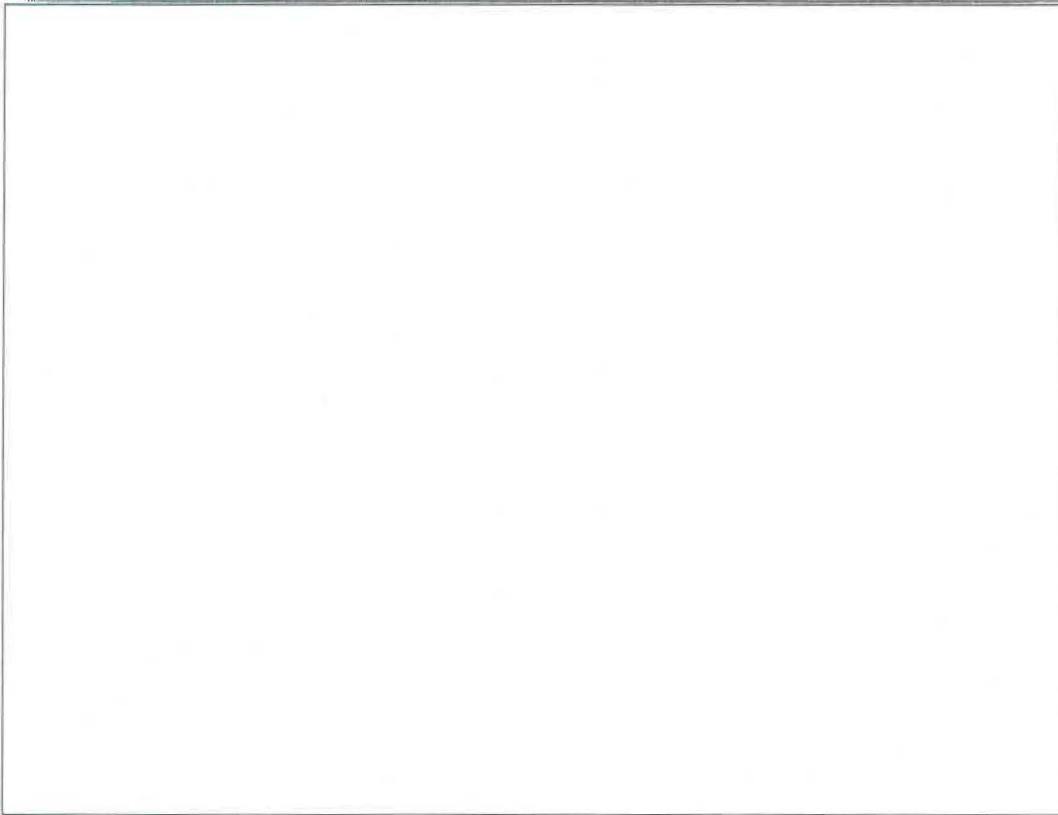
OFFICE OF GENERAL COUNSEL

UNCLASSIFIED // FOR OFFICIAL USE ONLY

49



Any Questions?



(b)(3)

OFFICE OF GENERAL COUNSEL

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

50

NATIONAL RECONNAISSANCE OFFICE

SUPRA ET ULTRA





NATIONAL RECONNAISSANCE OFFICE

14675 Lee Road
Chantilly, VA 20151-1715

20 July 2017

Human Rights Watch
350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
ATTN: Ms. Dinah PoKempner, General Counsel

REF: FOIA Case F-2017-00051

Dear Ms. PoKempner

This is in response to your request dated 18 January 2017, received in the National Reconnaissance Office (NRO) on 19 January 2017. Pursuant to the Freedom of Information Act (FOIA), you requested a copy of *"final or working policy and other documents that relate to the ability of the NRO to obtain access to communications and related data the U.S. government has acquired under 50 U.S.C §1881a...or Executive Order 12333..."*

Your request has been processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. A thorough search of our files and databases located ten documents responsive to your request. One document is being released to you in full; seven documents are being released in part; one document is being denied in full; and one document has been treated for NRO equities and is being referred to another agency for their further review and direct response to you.

Material withheld from release is denied pursuant to FOIA exemptions (b)(1), as properly classified information under Executive Order 13526, Section 1.4(c); and (b)(3), which is the basis for withholding information exempt from disclosure by statute. The relevant withholding statute is 10 U.S.C. § 424, which provides (except as required by the President or for information provided to Congress), that no provision of law shall be construed to require the disclosure of the organization or any function of the NRO; the number of persons employed by or assigned or detailed to the NRO; or the name or official title, occupational series, grade, or salary of any such person.

With regard to your early administrative appeal regarding denial of expedited processing, we processed your request as quickly as possible; we believe this response to your initial request essentially provides the remedy sought in your appeal, rendering an appellate determination regarding expedited processing unnecessary.


You are advised that you are entitled to a judicial review of this determination in a United States District Court in accordance with 5 U.S.C. § 522, as amended.

As part of the 2007 FOIA amendments, the Office of Government Information Services (OGIS) was created to offer mediation services to resolve disputes between FOIA (not Privacy Act) requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. You may contact OGIS in any of the following ways:

Office of Government Information Services
National Archives and Records Administration
Room 2510
8601 Adelphi Road
College Park, MD 20740-6001
E-mail: ogis@nara.gov
Telephone: 301-837-1996
Facsimile: 301-837-0348
Toll-free: 1-877-684-6448

If you have any questions, please call the Requester Service Center at (703) 227-9326 and reference case numbers **F-2017-00051**.

Sincerely,


Patricia B. Camerese
FOIA Public Liaison

Enclosures:

1. Intelligence Oversight Brief
2. NRO Directive 80-2
3. NRO Directive 80-4
4. NRO Directive 80-7
5. NRO Instruction 80-7-1
6. NRO Instruction 80-7-4
7. NRO Instruction 80-2-4
8. Office of the Director Policy Note 2015-1